SMC Networks

EliteConnect™

2.4GHz 802.11g Wireless Access Point

User Guide

SMC2552W-G

EliteConnect™ 2.4GHz 802.11g Wireless Access Point User Guide

The easy way to make all your network connections

SMC® Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

April 2004
Revision Number: R01, F2.0.22

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2004 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

All rights reserved.

Trademarks:
SMC is a registered trademark; and EliteConnect is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:
http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer’s expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968.

Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

COMPLIANCES

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Wireless 2.4 GHz Band Statements:

As the SMC2552W-G Access Point can operate in the 2412-2462 MHz frequency band it is limited by the FCC, Industry Canada and some other countries to indoor use only so as to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

The term “IC:” before the radio certification number only signifies that Industry Canada technical specifications were met.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: “Appareils Numériques,” NMB-003 édictée par l’Industrie.

Australia/New Zealand AS/NZS 4771

Contact SMC at:

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

EC Conformance Declaration CE0560!

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2º, 4ª,
08970 - Sant Joan Despí,
Barcelona, Spain.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950 (IEC 60950) - Product Safety
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device.
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.
- This device may be operated *indoors or outdoors* in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below.
  - In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
  - In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
  - In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing the switch:

WARNING: Installation and removal of the unit must be carried out by qualified personnel only.

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

France and Peru only

This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground).

† Impédance à la terre

Important! Before making connections, make sure you have the correct cord set.

Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	The minimum specifications for the flexible cord are: - No. 18 AWG - not longer than 2 meters, or 16 AWG. - Type SV or SJ - 3-conductor
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.

Power Cord Set	
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	The supply plug must comply with CEE7/7 (“SCHUKO”).
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	IEC-320 receptacle.

Veuillez lire à fond l'information de la sécurité suivante avant d'installer le Switch:

AVERTISSEMENT: L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.

- Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).
- Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes internationales de sécurité.
- Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN 60320/IEC 320.
- La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.
- L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.

France et Pérou uniquement:
Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

Cordon électrique - Il doit être agréé dans le pays d'utilisation	
Etats-Unis et Canada:	Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA.
	Les spe'cifications minimales pour un cable flexible sont AWG No. 18, ouAWG No. 16 pour un cable de longueur infe'rieure a` 2 me'tres. - type SV ou SJ - 3 conducteurs
	Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A.
	La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V).
Danemark:	La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.

Cordon électrique - Il doit être agréé dans le pays d'utilisation	
Suisse:	La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO") LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum).

Bitte unbedingt vor dem Einbauen des Switches die folgenden Sicherheitsanweisungen durchlesen (Germany):

WARNUNG: Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen.

- Das Gerät sollte nicht an eine ungeerdete Wechselstromsteckdose angeschlossen werden.
- Das Gerät muß an eine geerdete Steckdose angeschlossen werden, welche die internationalen Sicherheitsnormen erfüllt.
- Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß einen gemäß EN 60320/IEC 320 konfigurierten Geräteeingang haben.
- Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.
- Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur

gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.

Stromkabel**. Dies muss von dem Land, in dem es benutzt wird geprüft werden:**	
U.S.A und Canada	Der Cord muß das UL gepruft und war das CSA beglaubigt.
	Das Minimum spezifikation fur der Cord sind: - Nu. 18 AWG - nicht mehr als 2 meter, oder 16 AWG. - Der typ SV oder SJ - 3-Leiter
	Der Cord muß haben eine strombelastbarkeit aus wenigstens 10 A
	Dieser Stromstecker muß hat einer erdschluss mit der typ NEMA 5-15P (15A, 125V) oder NEMA 6-15P (15A, 250V) konfiguration.
Danemark	Dieser Stromstecker muß die ebene 107-2-D1, der standard DK2-1a oder DK2-5a Bestimmungen einhalten.
Schweiz	Dieser Stromstecker muß die SEV/ASE 1011Bestimmungen einhalten.
Europe	Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen. Der Netzstecker muß die Norm CEE 7/7 erfüllen (”SCHUKO”).

TABLE OF CONTENTS

1 Introduction 1-1

Package Checklist 1-2
Hardware Description 1-3
Component Description 1-4
Features and Benefits 1-7
Applications 1-8
System Defaults 1-9

2 Hardware Installation 2-1

3 Network Configuration 3-1

Network Topologies 3-2
Ad Hoc Wireless LAN (no AP or Bridge) 3-2
Infrastructure Wireless LAN 3-3
Infrastructure Wireless LAN for Roaming Wireless PCs . 3-4

4 Initial Configuration 4-1

Initial Setup through the CLI 4-1
Required Connections 4-1
Initial Configuration Steps 4-3
Using Web-based Management 4-4

5 System Configuration 5-1

Advanced Configuration 5-2
System Identification 5-4
TCP / IP Settings 5-6
Radius 5-9
Authentication 5-12
Filter Control 5-20
SNMP 5-25
Administration 5-28
System Log 5-34
Radio Interface 5-40
Radio Settings (802.11g) 5-41
Security 5-47
Status Information 5-61
Access Point Status 5-61
Station Status 5-64

Event Logs 5-66

6 Command Line Interface 6-1

Using the Command Line Interface 6-1
Accessing the CLI 6-1
Console Connection 6-1
Telnet Connection 6-2
Entering Commands 6-3
Keywords and Arguments 6-3
Minimum Abbreviation 6-4
Command Completion 6-4
Getting Help on Commands 6-4
Partial Keyword Lookup 6-5
Negating the Effect of Commands 6-6
Using Command History 6-6
Understanding Command Modes 6-6
Exec Commands 6-7
Configuration Commands 6-7
Command Line Processing 6-8
Command Groups 6-10
General Commands 6-11
configure 6-11
end 6-12
exit 6-12
ping 6-13
reset 6-14
show history 6-14
show line 6-15
System Management Commands 6-16
country 6-18
prompt 6-20
system name 6-20
username 6-21
password 6-22
ip http port 6-22
ip http server 6-23
logging on 6-24
logging host 6-24

logging console 6-25
logging level 6-26
logging facility-type 6-27
show logging 6-27
sntp-server ip 6-28
sntp-server enable 6-29
sntp-server date-time 6-30
sntp-server daylight-saving 6-31
sntp-server timezone 6-32
show sntp 6-32
show system 6-33
show version 6-34
SNMP Commands 6-35
snmp-server community 6-35
snmp-server contact 6-36
snmp-server enable server 6-37
snmp-server host 6-38
snmp-server location 6-39
show snmp 6-40
Flash/File Commands 6-40
bootfile 6-41
copy 6-42
delete 6-43
dir 6-44
RADIUS Client 6-45
radius-server address 6-46
radius-server port 6-46
radius-server key 6-47
radius-server retransmit 6-47
radius-server timeout 6-48
show radius 6-49
802.1x Port Authentication 6-50
802.1x 6-51
802.1x broadcast-key-refresh-rate 6-52
802.1x session-key-refresh-rate 6-53
802.1x session-timeout 6-54
address filter default 6-54
address filter entry 6-55

address filter delete 6-56
mac-authentication server 6-57
mac-authentication session-timeout 6-58
show authentication 6-59
Filtering Commands 6-60
filter local-bridge 6-60
filter ap-manage 6-61
filter ethernet-type enable 6-62
filter ethernet-type protocol 6-63
show filters 6-64
Interface Commands 6-65
interface 6-68
dns server 6-68
ip address 6-69
ip dhcp 6-71
shutdown 6-72
show interface ethernet 6-72
radio-mode 6-73
select-antenna-mode 6-74
description 6-75
ssid-broadcast 6-75
speed 6-76
channel 6-77
ssid 6-78
beacon-interval 6-78
dtim-period 6-79
fragmentation-length 6-80
rts-threshold 6-81
authentication 6-82
encryption 6-83
key 6-84
transmit-key 6-85
transmit-power 6-86
max-association 6-87
multicast-cipher 6-88
wpa-clients 6-89
wpa-mode 6-91
wpa-preshared-key 6-92

wpa-psk-type 6-93
shutdown 6-94
show interface wireless 6-95
show station 6-96
IAPP Commands 6-97
iapp 6-97
VLAN Commands 6-98
vlan 6-99
native-vlanid 6-100

A Troubleshooting A-1

Maximum Distance Table A-4

B Cables and Pinouts B-1

Twisted-Pair Cable Assignments B-1
10/100BASE-TX Pin Assignments B-2
Straight-Through Wiring B-3
Crossover Wiring B-3
Console Port Pin Assignments B-4
Wiring Map for Serial Cable B-4
Serial Cable Signal Directions for DB-9 Ports B-5

C Specifications C-1

General Specifications C-1
Sensitivity C-4
Transmit Power C-5

Glossary

Index

Chapter 1
Introduction

SMC's EliteConnect 2.4GHz 802.11g Wireless Access Point (SMC2552W-G) is an IEEE 802.11b/g access point that provides transparent, wireless high-speed data communications between the wired LAN and fixed, portable or mobile devices equipped with a 802.11b, or 802.11g wireless adapter.

This solution offers fast, reliable wireless connectivity with considerable cost savings over wired LANs (which include long-term maintenance overhead for cabling). Using 802.11b and 802.11g technology, this access point can easily replace a 10 Mbps Ethernet connection or seamlessly integrate into a 10/100 Mbps Ethernet LAN.

In addition, the access point offers full network management capabilities through an easy to configure web interface, a command line interface for initial configuration and troubleshooting, and support for Simple Network Management tools, such as SMC's EliteView.

Radio Characteristics – The IEEE 802.11g standard uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates at 2.4 GHz for connections to 802.11g clients.

IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard. IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) modulation technology to achieve a communication rate of up to 11 Mbps.

Package Checklist

The EliteConnect 2.4GHz 802.11g Wireless Access Point package includes:

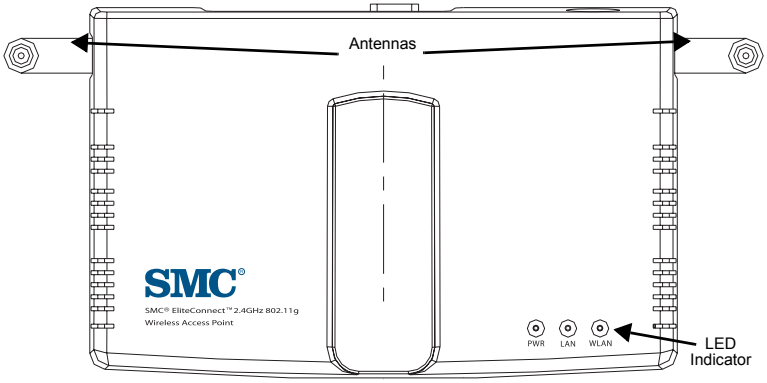
- One 2.4GHz 802.11g Wireless Access Point (SMC2552W-G)
- One Category 5 network cable
- One RS-232 console cable
- One AC power adapter and power cord
- One mounting bracket
- Four rubber feet
- Three wall-mount screws
- One Documentation CD
- This User Guide

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

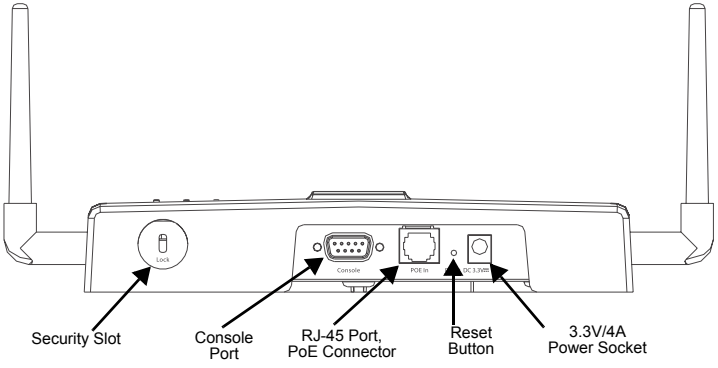
Please register this product and upgrade the product warranty at **www.smc.com**

Hardware Description

Front Panel



Rear Panel



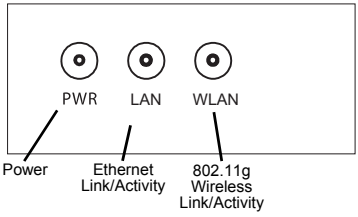
Component Description

Antennas

The access point includes two antennas for wireless communications. The signal transmitted from both antennas is identical, but only the best signal received on one of the antennas is used. The antennas transmit the outgoing signal as a toroidal sphere, so the antennas should be adjusted to different angles to provide better coverage. For further information, see “Positioning the Antennas” on page 2-3.

LED Indicators

The access point includes three status LED indicators, as described in the following figure and table.



LED	Status	Description
PWR	Off	No power.
	On Green	Power on and ready for operation.
	On Amber	H/W error or system error.
	Blinking Green (Slow)	Indicates one of the following: • running the power-on self-test • loading new software
LAN	Off	Indicates no valid Ethernet cable link on the RJ-45 port, or that the port has been administratively disabled
	On/Flashing Green	Indicates a valid 100 Mbps link on the RJ-45 port. Flashing indicates activity.
	On/Flashing Amber	Indicates a valid 10 Mbps link on the RJ-45 port. Flashing indicates activity.

LED	Status	Description
WLAN	Off	Indicates the 802.11b/g radio is administratively disabled.
	On Green	The access point is associated with wireless clients, but there is no network activity.
	Blinking Green	Indicates that the access point is transmitting or receiving data through wireless links.

Security Slot

The access point includes a Kensington security slot on the rear panel. You can prevent unauthorized removal of the access point by wrapping the Kensington security cable (not provided) around an unmovable object, inserting the lock into the slot, and turning the key.

Console Port

This port is used to connect a console device to the access point through a serial cable. This connection is described under “Console Port Pin Assignments” on page B-4. The console device can be a PC or workstation running a VT-100 terminal emulator, or a VT-100 terminal.

Ethernet Port

The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3 or 802.3u specifications.

This port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports.

However, when connecting the access point to a workstation or other device that does not have MDI-X ports, you must use crossover twisted-pair cable.

The access point appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to remote workstations on the wireless infrastructure.

Note: The RJ-45 port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. Refer to the description for the "Power Connector" for information on supplying power to the access point's network port from a network device, such as a switch, that provides Power over Ethernet (PoE).

Reset Button

This button is used to reset the access point or restore the factory default configuration. If you hold down the button for less than 5 seconds, the access point will perform a hardware reset. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the access point.

Power Connector

The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The access point automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

The access point may also receive Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard.

Note that if the access point is connected to a PoE source device and also connected to a local power source through the AC power adapter, PoE will be disabled.

Features and Benefits

- Local network connection via 10/100 Mbps Ethernet ports or 54 Mbps wireless interface (supporting up to 64 mobile users)
- IEEE 802.11b, 802.11g and 802.3af compliant
- Antennas with SMA connectors for optional external 2.4 GHz high-gain antenna to extend range and coverage
- Flexible network management through Command Line Interface (CLI), Web-based, Telnet, TFTP and SNMP, make it simple and easy to monitor, troubleshoot and remotely manage the network
- Power over Ethernet support reduces access point installation costs and provides centralised power management.
- Advanced security through 64/128/152-bit Wired Equivalent Privacy (WEP) encryption, IEEE 802.1x port authentication, Wi-Fi Protected Access (WPA), SSID broadcast disable, remote authentication via RADIUS server, and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network
- Provides seamless roaming within the WLAN service area
- Scans all available channels and selects the best channel for each client based on the signal-to-noise ratio

Applications

The Wireless products offer a high speed, reliable, cost-effective solution for 10/100 Mbps wireless Ethernet client access to the network in applications such as:

- **Remote access to corporate network information**
  E-mail, file transfer, and terminal emulation.
- **Difficult-to-wire environments**
  Historical or old buildings, asbestos installations, and open areas where wiring is difficult to employ.
- **Frequently changing environments**
  Retailers, manufacturers, and banks that frequently rearrange the workplace or change location.
- **Temporary LANs for special projects or peak times**
  Trade shows, exhibitions and construction sites which need temporary setup for a short time period. Retailers, airline and shipping companies that need additional workstations for a peak period. Auditors who require workgroups at customer sites.
- **Access to databases for mobile workers**
  Doctors, nurses, retailers, or white-collar workers who need access to databases while being mobile in a hospital, retail store, or an office campus.

System Defaults

The following table lists some of the access point's basic system defaults. To reset the access point defaults, use the CLI command "reset configuration" from the Exec level prompt.

Feature	Parameter	Default
Identification	System Name	Enterprise AP
Administration	User Name	admin
	Password	smcadmin
General	HTTP Server	Enabled
	HTTP Server Port	80
TCP/IP	DHCP	Enabled
	IP Address	192.168.2.2
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	Primary DNS IP	0.0.0.0
	Secondary DNS IP	0.0.0.0
RADIUS (Primary and Secondary)	IP Address	0.0.0.0
	Port	1812
	Key	DEFAULT
	Timeout	5 seconds
	Retransmit attempts	3

Feature	Parameter	Default
MAC Authentication	MAC	Local MAC
	Authentication Session Timeout	0 seconds (disabled)
	Local MAC System Default	Allowed
	Local MAC Permission	Allowed
802.1x Authentication	Status	Disabled
	Broadcast Key Refresh	0 minutes (disabled)
	Session Key Refresh	0 minutes (disabled)
	Reauthentication Refresh Rate	0 seconds (disabled)
VLAN	Native VLAN ID	1
	VLAN Tag Support	Disabled
Filter Control	Local Bridge	Disabled
	Local Management	Disabled
	Ethernet Type	Disabled
SNMP	Status	Enabled
	Location	null
	Contact	Contact
	Community (Read Only)	Public
	Community (Read/Write)	Private
	Traps	Enabled
	Trap Destination IP Address	null
	Trap Destination Community Name	Public

Feature	Parameter	Default
System Logging	Syslog	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Informational
	Logging Facility Type	16
Ethernet Interface	Speed and Duplex	Auto
Wireless Interface 802.11b/g	IAPP	Enabled
	SSID	SMC
	Status	Enabled
	Auto Channel Select	Enabled
	SSID Broadcast	Disabled
	Transmit Power	Full
	Maximum Data Rate	54 Mbps
	Beacon Interval	100 TUs
	Data Beacon Rate (DTIM Interval)	2 beacons
	RTS Threshold	2347 bytes

Feature	Parameter	Default
Wireless Security 802.11b/g	Authentication Type	Open System
	WEP Encryption	Disabled
	WEP Key Length	128 bits
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	null
	WPA Configuration Mode	All clients
	WPA Key Management	WPA authentication over 802.1x
	Multicast Cipher	WEP

Chapter 2
Hardware Installation

1. **Select a Site** – Choose a proper place for the access point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. Try to place the access point in a position that can best cover its Basic Service Set (refer to “Infrastructure Wireless LAN” on page 3-3). Normally, the higher you place the access point, the better the performance.

2. **Mount the Access Point** – The access point can be mounted on any horizontal surface or wall. You can mount the access point on a wall as shown in the illustrations on the next page.

   Mounting on a horizontal surface – To keep the access point from sliding on the surface, attach the four rubber feet provided in the accessory kit to the embossed circles on the bottom of the access point.

   Mounting on a wall – The access point should be mounted only to a wall or wood surface that is at least 1/2-inch plywood or its equivalent.

   Position the mounting bracket on the wall, and mark the holes. The orientation shown in the following figure is the most secure position for mounting the access point. Do not mount the access point with the retaining latches pointing down.

   To mount the access point on a plastered brick or concrete wall, first drill four holes 22 mm deep and 3.5 mm in diameter, and press the four included wall plugs firmly into the drilled holes until they are flush with the surface of the wall.

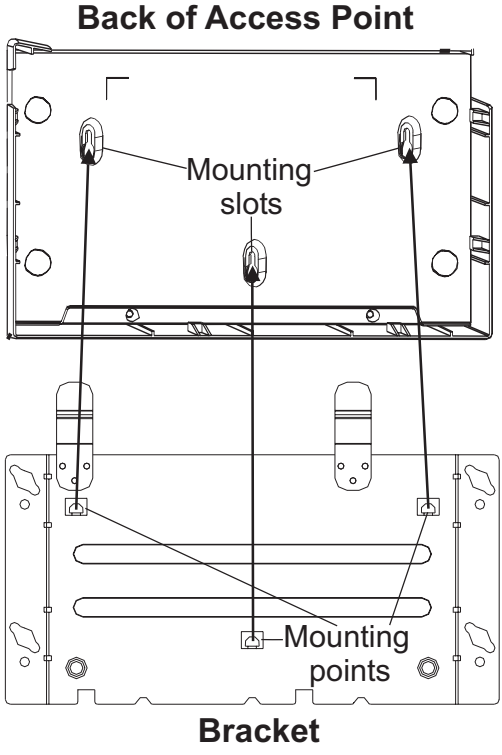
Set the four 5/8-inch number 12 wood screws in the holes, leaving about 3 mm clearence from the wall.

Position the mounting bracket over the wall screws, slide the bracket onto the screws, and then tighten down the screws.

3. **Attaching the Bracket** – Line up the three mounting points on the bracket with the three mounting slots on the rear of the access point, as directed in the figure on the next page.

   Place the mounting points of the bracket into the mounting slots of the access point and while pushing down on the bracket, slide it into position so that the two retaining latches slip into place over the back of the access point.

Attaching the Mounting Bracket



4. **Lock the Access Point in Place** – To prevent unauthorized removal of the access point, you can use a Kensington Slim MicroSaver security cable (not included) to attach the access point to a fixed object.

5. **Connect the Power Cord** – Connect the power adapter to the access point, and the power cord to an AC power outlet.

   Otherwise, the access point can derive its operating power directly from the RJ-45 port when connected to a device that provides IEEE 802.3af compliant Power over Ethernet (PoE).

   Note: If the access point is connected to both a PoE source device and an AC power source, PoE will be disabled.

   Warning: Use ONLY the power adapter supplied with this access point. Otherwise, the product may be damaged.

6. **Observe the Self Test** – When you power on the access point, verify that the PWR indicator stops flashing and remains on, and that the other indicators start functioning as described under “LED Indicators” on page 1-4.

   If the PWR LED does not stop flashing, the self test has not completed correctly. Refer to “Troubleshooting” on page A-1.

7. **Connect the Ethernet Cable** – The access point can be wired to a 10/100 Mbps Ethernet through a network device such as a hub or a switch. Connect your network to the RJ-45 port on the back panel with category 3, 4, or 5 UTP Ethernet cable. When the access point and the connected device are powered on, the LAN LED should light indicating a valid network connection.

   Note: The RJ-45 port on the access point uses an MDI pin configuration, so you must use straight-through cable for network connections to hubs or switches that only have MDI-X ports, and crossover cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDI/MDI-X operation, you can use either straight-through or crossover cable.

8. **Position the Antennas** – The antennas emit signals along a toroidal plane, and thus provide more effective coverage when positioned along different axes. For example, you might

position the antennas around 45 to 90 degrees from each other.

The access point also compares the strength of an incoming signal on both antennas, and uses the antenna receiving the stronger signal to communicate with a wireless client.

9. **Connect the Console Port** – Connect the console cable (included) to the RS-232 console port for accessing the command-line interface. You can manage the access point using the console port (Chapter 6), the web interface (Chapter 5), or SNMP management software such as SMC's EliteView.

Chapter 3
Network Configuration

The wireless solution supports a stand-alone wireless network configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs.

Wireless network cards, adapters, and access points can be configured as:

- Ad hoc for departmental, or enterprise LANs
- Infrastructure for wireless LANs
- Infrastructure wireless LAN for roaming wireless PCs

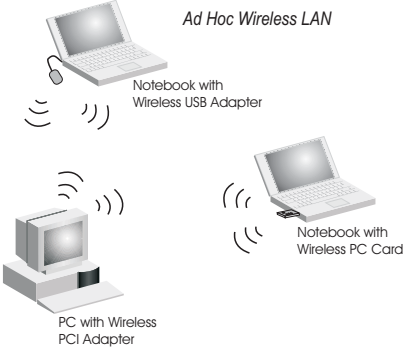
The 802.11b and 802.11g frequency band which operates at 2.4 GHz can easily encounter interference from other 2.4 GHz devices, such as other 802.11b or g wireless devices, cordless phones and microwave ovens. If you experience poor wireless LAN performance, try the following measures:

- Limit any possible sources of radio interference within the service area
- Increase the distance between neighboring access points
- Decrease the signal strength of neighboring access points
- Increase the channel separation of neighboring access points (e.g., up to 3 channels of separation for 802.11b or up to 5 channels for 802.11g)

Network Topologies

Ad Hoc Wireless LAN (no AP or Bridge)

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel.

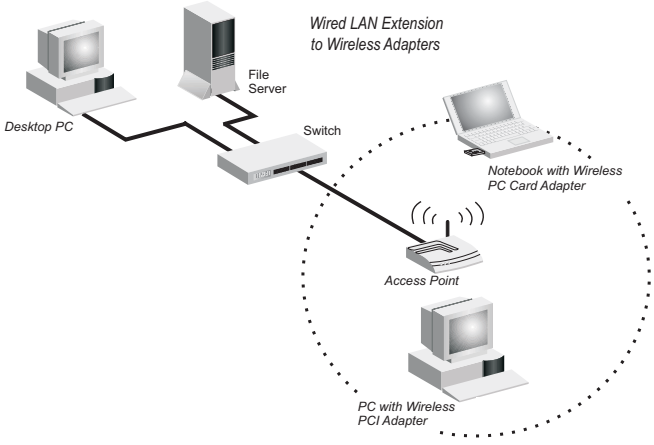


Infrastructure Wireless LAN

The access point also provides access to a wired LAN for wireless workstations. An integrated wired/wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can talk to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via the access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.

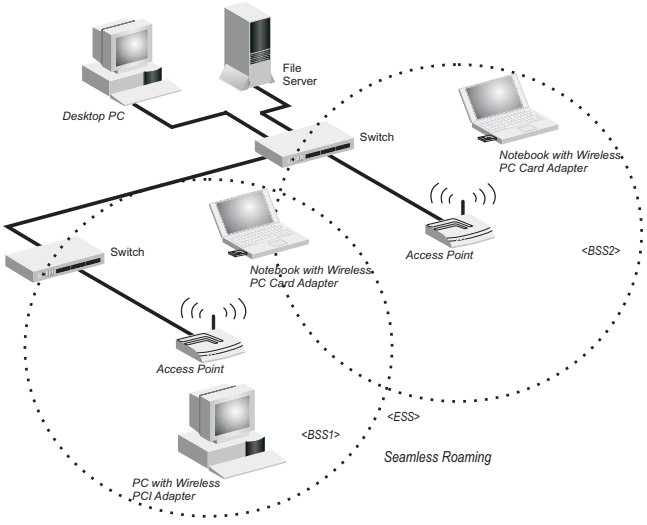


Infrastructure Wireless LAN for Roaming Wireless PCs

The Basic Service Set (BSS) defines the communications domain for each access point and its associated wireless clients. The BSS ID is a 48-bit binary number based on the access point's wireless MAC address, and is set automatically and transparently as clients associate with the access point. The BSS ID is used in frames sent between the access point and its clients to identify traffic in the service area.

The BSS ID is only set by the access point, never by its clients. The clients only need to set the Service Set Identifier (SSID) that identifies the service set provided by one or more access points. The SSID can be manually configured by the clients, can be detected in an access point's beacon, or can be obtained by querying for the identity of the nearest access point. For clients that do not need to roam, set the SSID for the wireless card to that used by the access point to which you want to connect.

A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All SMC wireless network cards and adapters and SMC2552W-G wireless access points within a specific ESS must be configured with the same SSID.



Chapter 4
Initial Configuration

The EliteConnect 2.4GHz 802.11g Wireless Access Point SMC2552W-G offers a variety of management options, including a web-based interface, a direct connection to the console port, or using SNMP software such as SMC's EliteView.

The initial configuration steps can be made through the web browser interface using the Setup Wizard (page 4-4). The access point requests an IP address via DHCP by default. If no response is received from a DHCP server, then the access point uses the default address 192.168.2.2. You can also use the command line interface (CLI) as described below to configure a valid address.

Note: Units sold in countries outside the United States are not configured with a specific country code. You must use the CLI to set the country code and enable wireless operation (page 4-4).

Initial Setup through the CLI

Required Connections

The SMC2552W-G provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuration. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the access point. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown on page B-4.

To connect to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the access point.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or 2).
   - Set the data rate to 9600 baud.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

   Note: When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.
4. Once you have set up the terminal correctly, press the [Enter] key to initiate the console connection. The console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 6-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 6-10.

Initial Configuration Steps

Logging In – Enter “admin” for the user name. The default password is “smcadmin”. The CLI prompt appears displaying “SMC Enterprise AP#.”

```
Username: admin
Password: smcadmin
SMC Enterprise AP#
```

Setting the IP Address – By default, the access point is configured to obtain IP address settings from a DHCP server. You may also use the command line interface (CLI) to assign an IP address that is compatible with your network.

Type “configure” to enter configuration mode, then type “interface ethernet” to access the Ethernet interface-configuration mode.

```
SMC Enterprise AP#configure
SMC Enterprise AP(config)#interface ethernet
SMC Enterprise AP(config-if)#
```

First type “no dhcp” to disable DHCP client mode. Then type “ip address *ip-address netmask gateway*,” where “ip-address” is the access point’s IP address, “netmask” is the network mask for the network, and “gateway” is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network.

```
SMC Enterprise AP(if-ethernet)#no dhcp
SMC Enterprise AP(if-ethernet)#ip address 192.168.2.2
   255.255.255.0 192.168.2.254
SMC Enterprise AP(if-ethernet)#
```

After configuring the access point’s IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be

accessed using Telnet from any computer attached to the network.

Setting the Country Code – Units sold in the United States are configured by default to use only radio channels 1-11 as defined by FCC regulations. Units sold in other countries are configured by default without a country code (i.e., 99). You must use the CLI to set the country code. Setting the country code restricts operation of the access point to the radio channels permitted for wireless networks in the specified country.

Type “exit” to leave configuration mode. Then type “country?” to display the list of countries. Select the code for your country, and enter the country command again, following by your country code (e.g., IE for Ireland).

```
SMC Enterprise AP#country ie
SMC Enterprise AP#
```

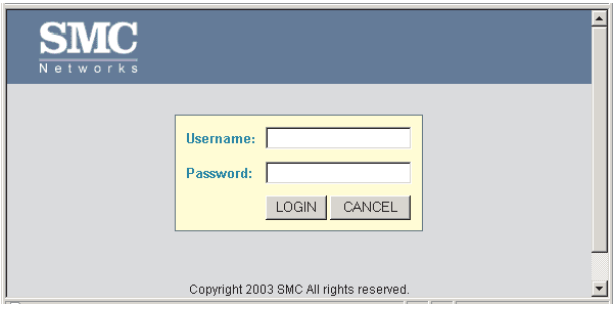
Using Web-based Management

Setup Wizard

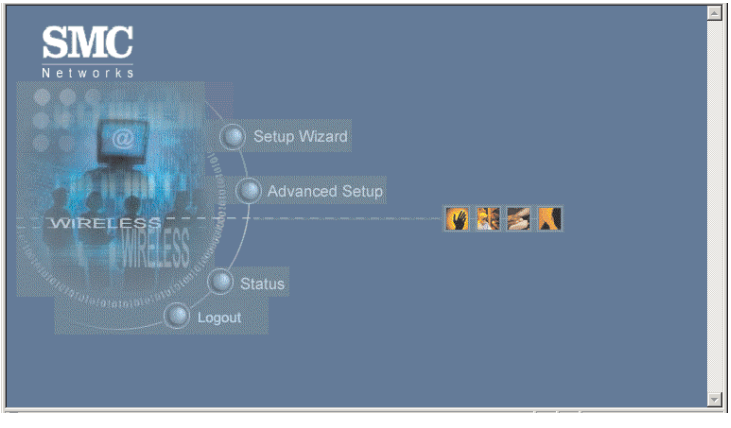
There are only a few basic steps you need to complete to connect the SMC2552W-G to your corporate network, and provide network access to wireless clients. The Setup Wizard takes you through configuration procedures for the wireless Service Set Identifier, the radio channel selection and IP configuration.

The SMC2552W-G can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). Enter your configured IP address or the default IP address: http://192.168.2.2

Logging In – Enter the username “admin,” the password “smcadmin,” and click LOGIN. For information on configuring a user name and password, refer to page 5-28.

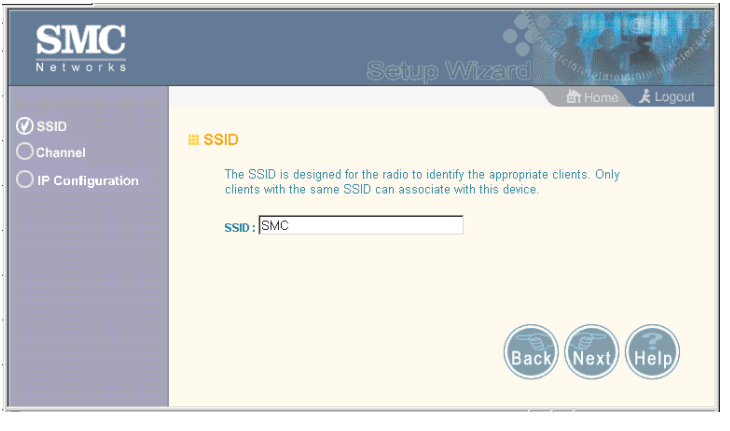


The home page displays the Main Menu.



Launching the Setup Wizard – To perform initial configuration, click Setup Wizard on the home page, then click on the [Next] button to start the process.

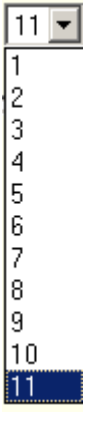
1. **Service Set ID** – Enter the service set identifier in the SSID box which all wireless clients must use to associate with the access point. The SSID is case sensitive and can consist of up to 32 alphanumeric characters.
   (Default: SMC)



2. **Radio Channel** – You must enable radio communications for 802.11b and 802.11b/g, and set the operating radio channel.

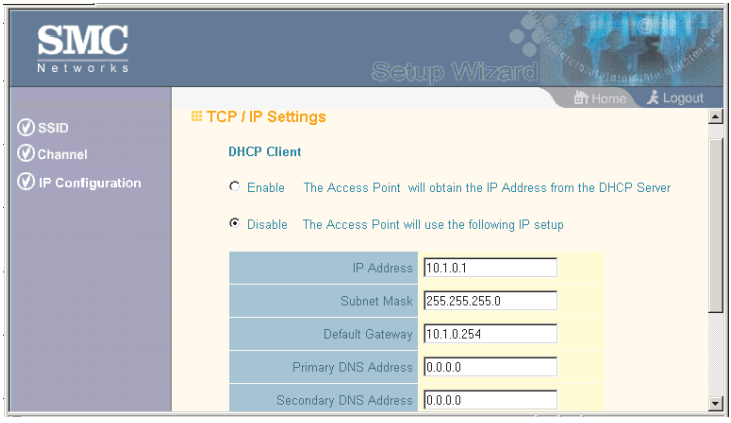
Auto Channel Select – Select Enable for automatic radio channel detection. (Default: Enable)

802.11g Radio Channel: Set the operating radio channel number. (Range: 1-11)



Note: Available channel settings are limited by local regulations which determine which channels are available. (See “Maximum Channels” on page C-1.)

3. **IP Configuration** – Either enable or disable (Dynamic Host Configuration Protocol (DHCP) for automatic IP configuration. If you disable DHCP, then manually enter the IP address and subnet mask. If a management station exists on another network segment, then you must enter the IP address for a gateway that can route traffic between these segments. Then enter the IP address for the primary and secondary Domain Name Servers (DNS) servers to be used for host-name to IP address resolution.



DHCP Client – With DHCP Client enabled, the IP address, subnet mask and default gateway can be dynamically assigned to the access point by the network DHCP server. (Default: Enable)

Note: If there is no DHCP server on your network, then the access point will automatically start up with its default IP address, 192.168.2.2.

4. Click Finish.

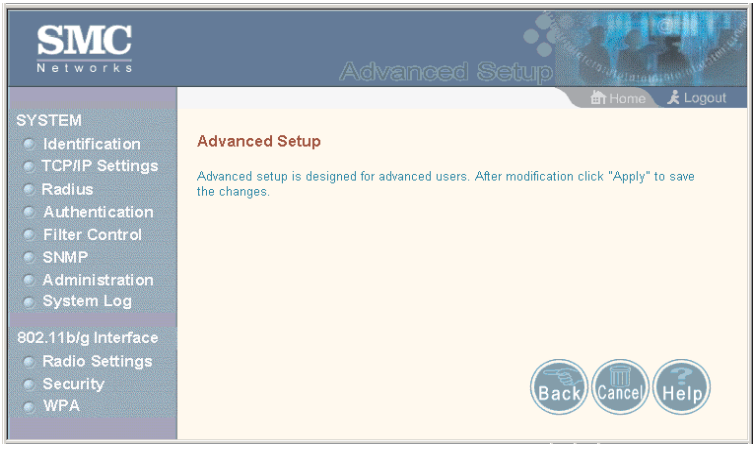
5. Click the OK button to restart the access point.

Chapter 5
System Configuration

Before continuing with advanced configuration, first complete the initial configuration steps described in Chapter 4 to set up an IP address for the SMC2552W-G.

The SMC2552W-G can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above). The SMC2552W-G Access Point is DHCP enabled by default.

To log into the SMC2552W-G, enter the default user name “admin” and password “smcadmin.” When the home page displays, click on Advanced Setup. The following page will display.



The information in this chapter is organized to reflect the structure of the web screens for easy reference. However, we recommend that you configure a user name and password as the first step under advanced configuration to control management access to this device (page 5-28).

Advanced Configuration

The Advanced Configuration pages include the following options.

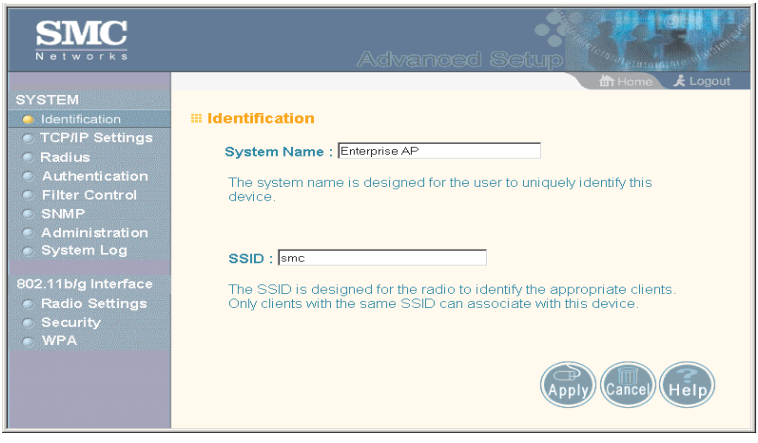
Menu	Description	Page
System	Configures basic administrative and client access	5-4
Identification	Specifies the host name and Service Set Identifier (SSID)	5-4
TCP / IP Settings	Configures the IP address, subnet mask, gateway, and domain name servers	5-6
Radius	Configures the RADIUS server for wireless client authentication	5-9
Authentication	Configures 802.1x client authentication, with an option for MAC address authentication	5-12
Filter Control	Filters communications between wireless clients, access to the management interface from wireless clients, and traffic matching specific Ethernet protocol types	5-20
SNMP	Controls access to this access point from management stations using SNMP, as well as the hosts that will receive trap messages	5-25
Administration	Configures user name and password for management access; upgrades software from local file, FTP or TFTP server; resets configuration settings to factory defaults; and resets the access point	5-28
System Log	Controls logging of error messages; sets the system clock via SNTP server or manual configuration	5-34

Menu	Description	Page
802.11b/g Interface	Configures the IEEE 802.11b/g interface	5-40
Radio Settings	Configures radio signal parameters, such as radio channel, transmission rate, and beacon settings	5-41
Security	Configures data encryption with Wired Equivalent Protection (WEP)	5-47
WPA	Configures advanced encryption and authentication with Wi-Fi Protected Access (WPA)	5-45

System Identification

The system information parameters for the SMC2552W-G can be left at their default settings. However, modifying these parameters can help you to more easily distinguish different devices in your network.

You should set a Service Set Identification (SSID) to identify the wireless network service provided by the SMC2552W-G. Only clients with the same SSID can associate with the access point.



System Name – An alias for the access point, enabling the device to be uniquely identified on the network. (Default: Enterprise AP; Range: 1-22 characters)

SSID – The name of the basic service set provided by the access point. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point. (Default: SMC; Range: 1-32 characters, case sensitive)

CLI Commands for System Identification – Enter the global configuration mode, and use the **system name** command to specify a new system name. Enter the wireless configuration mode (11g), and use the **ssid** command to set the service set identifier. Then return to the Exec mode, and use the **show system** command to display the changes to the system identification settings**.**

```
SMC AP#configure                                                    6-11
SMC-AP(config)#system name R&D                                      6-20
SMC-AP(config)#interface wireless g                                 6-68
SMC-AP(if-wireless g)#ssid r&d                                      6-78
SMC-AP(if-wireless g)#end                                           6-12
SMC-AP#show system                                                  6-33

System Information
================================================
Serial Number        : A324003220
System Up time       : 0 days, 0 hours, 32 minutes, 51 seconds
System Name          : r&d
System Location      :
System Contact       : Contact
System Country Code  : US - UNITED STATES
MAC Address          : 00-30-F1-91-91-5B
IP Address           : 192.168.2.51
Subnet Mask          : 255.255.255.0
Default Gateway      : 192.168.2.250
VLAN State           : DISABLED
Native VLAN ID       : 1
IAPP State           : ENABLED
DHCP Client          : ENABLED
HTTP Server          : ENABLED
HTTP Server Port     : 80
Slot Status          : Band(g)
Software Version     : v2.0.22
================================================

SMC-AP#
```

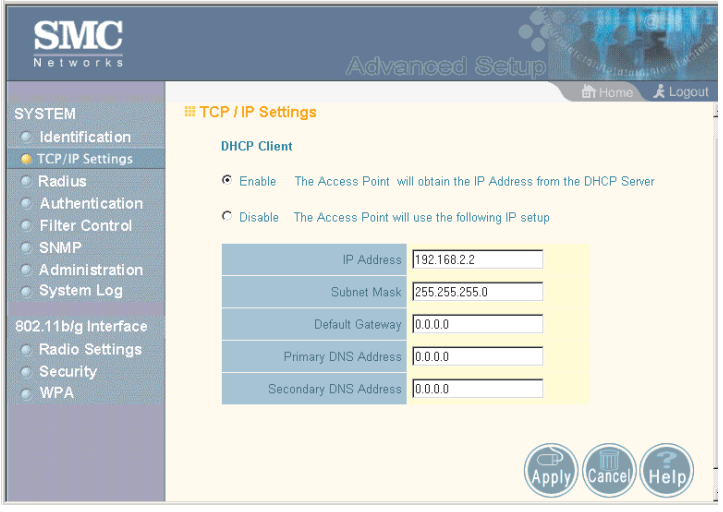
TCP / IP Settings

Configuring the SMC2552W-G with an IP address expands your ability to manage the access point. A number of access point features depend on IP addressing to operate.

Note: You can use the web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network.

By default, the SMC2552W-G will be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values (page 4-3). After you have network access to the access point, you can use the web browser interface to modify the initial IP configuration, if needed.

Note: If there is no DHCP server on your network, or DHCP fails, the access point will automatically start up with a default IP address of 192.168.2.2.



DHCP Client (Enable) – Select this option to obtain the IP settings for the access point from a DHCP (Dynamic Host Configuration Protocol) server. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to the access point by the network DHCP server. (Default: Enable)

DHCP Client (Disable) – Select this option to manually configure a static address for the access point.

- IP Address: The IP address of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- Subnet Mask: The mask that identifies the host address bits used for routing to specific subnets.
- Default Gateway: The default gateway is the IP address of the router for the access point, which is used if the requested destination address is not on the local subnet.

  If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.0).
- Primary and Secondary DNS Address: The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

  If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0).

CLI Commands for TCP/IP Settings – From the global configuration mode, enter the interface configuration mode with the **interface ethernet** command. Use the **ip dhcp** command to enable the DHCP client, or **no ip dhcp** to disable it. To manually configure an address, specify the new IP address, subnet mask, and default gateway using the **ip address** command. To specify DNS server addresses use the **dns server** command. Then use the **show interface ethernet** command from the Exec mode to display the current IP settings.

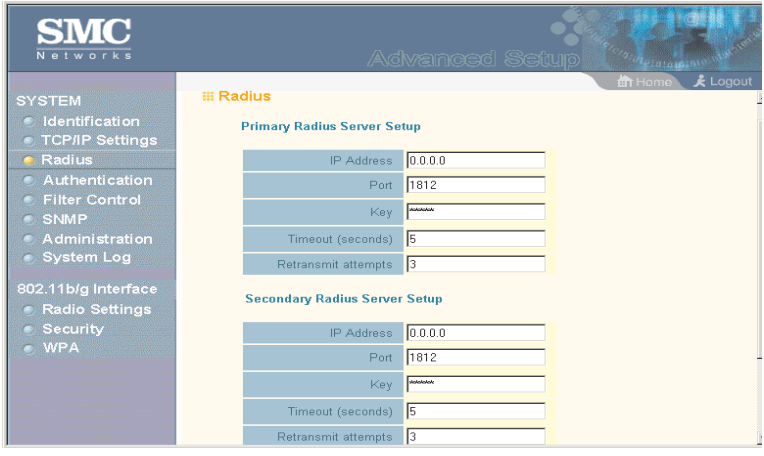
```
SMC-AP(config)#interface ethernet                          6-68
Enter Ethernet configuration commands, one per line.
SMC-AP(if-ethernet)#no ip dhcp                             6-71
SMC-AP(if-ethernet)#ip address 192.168.1.2
   255.255.255.0 192.168.1.253                             6-69
SMC-AP(if-ethernet)#dns primary-server 192.168.1.55        6-68
SMC-AP(if-ethernet)#dns secondary-server 10.1.0.55         6-68
SMC-AP(config)#end                                         6-12
SMC-AP#show interface ethernet                             6-72
Ethernet Interface Information
=======================================
IP Address           : 192.168.2.2
Subnet Mask          : 255.255.255.0
Default Gateway      : 192.168.1.253
Primary DNS          : 192.168.1.55
Secondary DNS        : 10.1.0.55
Admin status         : Up
Operational status   : Up
=======================================
SMC-AP#
```

Radius

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

A primary RADIUS server must be specified for the SMC2552W-G to implement IEEE 802.1x network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. If using WPA (PSK) mode then no RADIUS configuration is necessary. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.



Primary Radius Server Setup – Configure the following settings to use RADIUS authentication on the access point.

- IP Address: Specifies the IP address or host name of the RADIUS server.
- Port: The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- Key: A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- Timeout: Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5)
- Retransmit attempts: The number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3)

Note: For the Timeout and Retransmit attempts fields, accept the default values unless you experience problems connecting to the RADIUS server over the network.

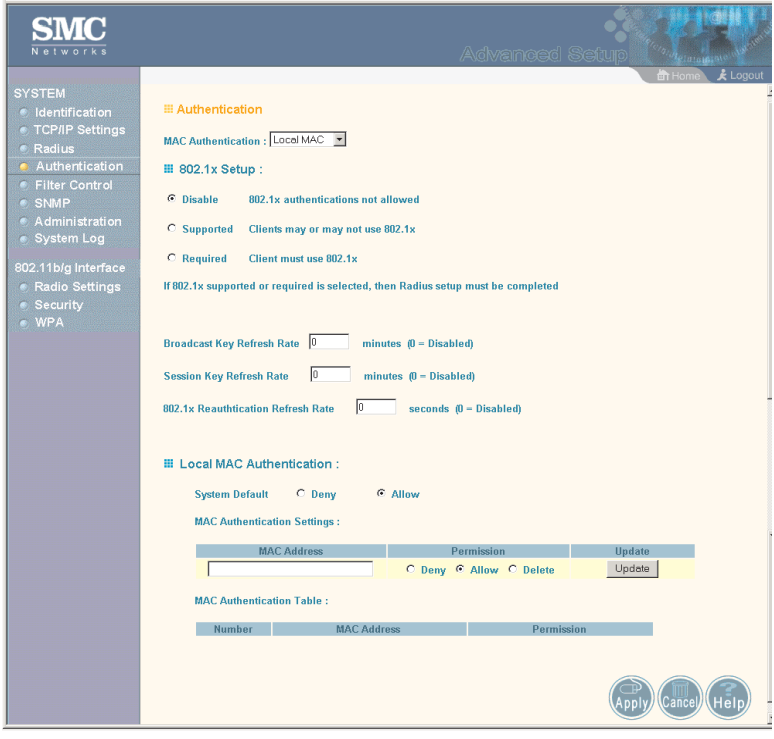
Secondary Radius Server Setup – Configure a secondary RADIUS server to provide a backup in case the primary server fails. The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role.

CLI Commands for RADIUS – From the global configuration mode, use the **radius-server address** command to specify the address of the primary or secondary RADIUS servers. (The following example configures the settings for the primary RADIUS server.) Configure the other parameters for the RADIUS server. Then use the **show show radius** command from the Exec mode to display the current settings for the primary and secondary RADIUS servers.

```
SMC-AP(config)#radius-server address 192.168.1.25      6-46
SMC-AP(config)#radius-server port 181                  6-46
SMC-AP(config)#radius-server key green                 6-47
SMC-AP(config)#radius-server timeout 10                6-48
SMC-AP(config)#radius-server retransmit 5              6-47
SMC-AP(config)#exit
SMC-AP#show radius                                     6-49

Radius Server Information
=========================================
IP               : 192.168.1.25
Port             : 181
Key              : *****
Retransmit       : 5
Timeout          : 10
=========================================

Radius Secondary Server Information
=========================================
IP               : 0.0.0.0
Port             : 1812
Key              : *****
Retransmit       : 3
Timeout          : 5
=========================================
SMC-AP#
```

Authentication

Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point, or by looking up their MAC addresses on a RADIUS server. The 802.1x protocol can also be configured to check other user credentials such as a user name and password.



MAC Authentication – You can configure a list of the MAC addresses for wireless clients that are authorized to access the network. This provides a basic level of authentication for wireless clients attempting to gain access to the network. A database of authorized MAC addresses can be stored locally on the SMC2552W-G or remotely on a central RADIUS server. (Default: Local MAC)

- Local MAC: The MAC address of the associating station is compared against the local database stored on the access point. The Local MAC Authentication section enables the local database to be set up.
- Radius MAC: The MAC address of the associating station is sent to a configured RADIUS server for authentication. When using a RADIUS authentication server for MAC address authentication, the server must first be configured in the Radius window (page 5-9).
- Disable: No checks are performed on an associating station's MAC address.

Local MAC Authentication – Configures the local MAC authentication database. The MAC database provides a mechanism to take certain actions based on a wireless client's MAC address. The MAC list can be configured to allow or deny network access to specific clients.

- System Default: Specifies a default action for all unknown MAC addresses (that is, those not listed in the local MAC database).
    - Deny: Blocks access for all MAC addresses except those listed in the local database as "allowed."
    - Allow: Permits access for all MAC addresses except those listed in the local database as "denied."

- MAC Authentication Settings: Enters specified MAC addresses and permissions into the local MAC database.
  - MAC Address: Physical address of a client. Enter six pairs of hexadecimal digits separated by hyphens; for example, 00-90-D1-12-AB-89.
  - Permission: Select Allow to permit access or Deny to block access. If Delete is selected, the specified MAC address entry is removed from the database.
  - Update: Enters the specified MAC address and permission setting into the local database.
- MAC Authentication Table: Displays current entries in the local MAC database.

Note: Client station MAC authentication occurs prior to the IEEE 802.1x authentication procedure configured for the access point. However, a client's MAC address provides relatively weak user authentication, since MAC addresses can be easily captured and used by another station to break into the network. Using 802.1x provides more robust user authentication using user names and passwords or digital certificates. So, although you can configure the access point to use MAC address and 802.1x authentication together, it is better to choose one or the other, as appropriate.

802.1x Setup – IEEE 802.1x is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1x client application to submit user credentials for authentication. The 802.1x standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants client access to the network.

The 802.1x EAP packets are also used to pass dynamic unicast session keys and static broadcast keys to wireless clients. Session keys are unique to each client and are used to encrypt and correlate traffic passing between a specific client and the access point. You can also enable broadcast key rotation, so the access point provides a dynamic broadcast key and changes it at a specified interval.

You can enable 802.1x as optionally supported or as required to enhance the security of the wireless network.

- Disable: The access point does not support 802.1x authentication for any wireless client. After successful wireless association with the access point, each client is allowed to access the network.
- Supported: The access point supports 802.1x authentication only for clients initiating the 802.1x authentication process (i.e., the access point does not initiate 802.1x authentication). For clients initiating 802.1x, only those successfully authenticated are allowed to access the network. For those clients not initiating 802.1x, access to the network is allowed after successful wireless association with the access point.
- Required: The access point enforces 802.1x authentication for all associated wireless clients. If 802.1x authentication is not initiated by a client, the access point will initiate authentication. Only those clients successfully authenticated with 802.1x are allowed to access the network.

When 802.1x is enabled, the broadcast and session key rotation intervals can also be configured.

- Broadcast Key Refresh Rate: Sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying. (Range: 0-1440 minutes; Default: 0 means disabled)

- Session Key Refresh Rate: The interval at which the access point refreshes unicast session keys for associated clients. (Range: 0-1440 minutes; Default: 0 means disabled)
- 802.1x Re-authentication Refresh Rate: The time period after which a connected client must be re-authenticated. During the re-authentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if re-authentication fails is network access blocked. (Range: 0-65535 seconds; Default: 0 means disabled)

CLI Commands for Local MAC Authentication – Use the **mac-authentication server** command from the global configuration mode to enable local MAC authentication. Set the default for MAC addresses not in the local table using the **address filter default** command, then enter MAC addresses in the local table using the **address filter entry** command. To remove an entry from the table, use the **address filter delete** command. To display the current settings, use the **show authentication** command from the Exec mode.

```
SMC-AP(config)#mac-authentication server local                  6-57
SMC-AP(config)#address filter default denied                    6-54
SMC-AP(config)#address filter entry 00-70-50-cc-99-1a denied    6-55
SMC-AP(config)#address filter entry 00-70-50-cc-99-1b allowed   6-55
SMC-AP(config)#address filter entry 00-70-50-cc-99-1c allowed   6-55
SMC-AP(config)#address filter delete 00-70-50-cc-99-1c          6-56
SMC-AP(config)#exit
SMC-AP#show authentication                                      6-59

Authentication Information
=========================================================
MAC Authentication Server      : LOCAL
MAC Auth Session Timeout Value : 300 secs
802.1x                         : DISABLED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1x Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address             Status
-----------------       ----------
00-70-50-cc-99-1a       DENIED
00-70-50-cc-99-1b       ALLOWED
=========================================================
SMC-AP#
```

CLI Commands for RADIUS MAC Authentication – Use the **mac-authentication server** command from the global configuration mode to enable remote MAC authentication. Set the timeout value for re-authentication using the **mac-authentication session-timeout** command. Be sure to also configure connection settings for the RADIUS server (not shown in the following example). To display the current settings, use the **show authentication** command from the Exec mode.

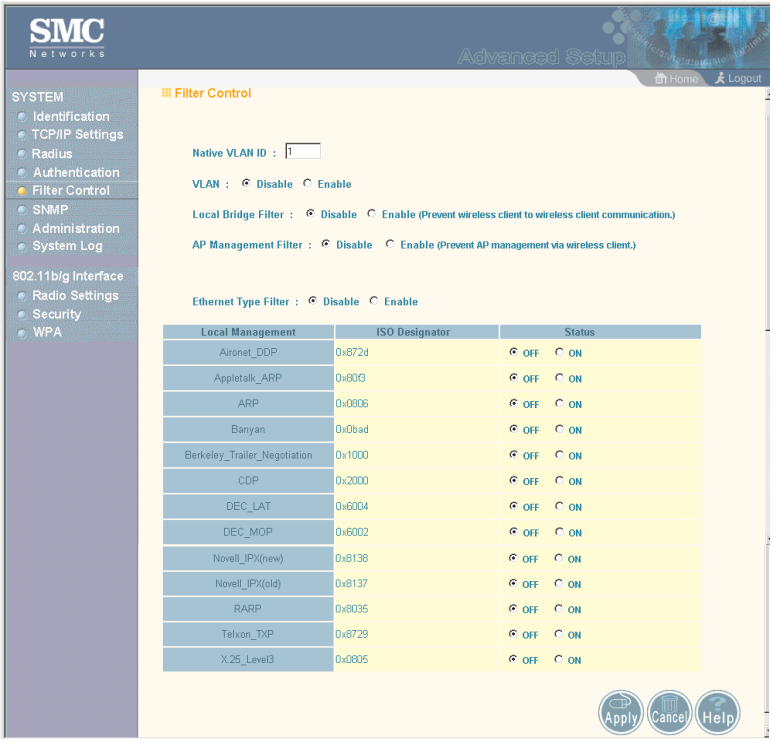
```
SMC-AP(config)#mac-authentication server remote        6-57
SMC-AP(config)#mac-authentication session-timeout 300  6-58
SMC-AP(config)#exit
SMC-AP#show authentication                             6-59

Authentication Information
============================================================
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 secs
802.1x                         : DISABLED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1x Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address             Status
-----------------       ----------
00-70-50-cc-99-1a       DENIED
00-70-50-cc-99-1b       ALLOWED
============================================================
SMC-AP#
```

CLI Commands for 802.1x Authentication – Use the **802.1x supported** command from the global configuration mode to enable 802.1x authentication. Set the session and broadcast key refresh rate, and the re-authentication timeout. To display the current settings, use the **show authentication** command from the Exec mode.

```
SMC-AP(config)#802.1x supported                          6-51
SMC-AP(config)#802.1x broadcast-key-refresh-rate 5       6-52
SMC-AP(config)#802.1x session-key-refresh-rate 5         6-53
SMC-AP(config)#802.1x session-timeout 300                6-54
SMC-AP(config)#exit
SMC-AP#show authentication                               6-59

Authentication Information
============================================================
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 300 secs
802.1x                         : SUPPORTED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1x Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address             Status
-----------------       ----------
00-70-50-cc-99-1a       DENIED
00-70-50-cc-99-1b       ALLOWED
============================================================
SMC-AP#
```

Filter Control

The access point can employ VLAN ID and network traffic frame filtering to control access to network resources and increase security.



Native VLAN ID – The VLAN ID assigned to wireless clients that are not assigned to a specific VLAN by RADIUS server configuration.

VLAN – Enables or disables VLAN tagging support on the SMC2552W-G. If enabled, the access point will tag traffic passing from wireless clients to the wired network with the VLAN ID associated with each client on the RADIUS server. Up to 16

VLAN IDs can be mapped to specific wireless clients, allowing users to remain within the same VLAN as they move around a campus site. This feature can also be used to control access to network resources from wireless clients, thereby improving security.

A VLAN ID (1-4095) is assigned to a client after successful authentication using IEEE 802.1x and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the access point assigns the user to its own configured native VLAN ID.

When setting up VLAN IDs for each user on the RADIUS server, be sure to use the RADIUS attributes and values as indicated in the following table.

Number	**RADIUS Attribute**	**Value**
64	Tunnel-Type	VLAN (13)
65	Tunnel-Medium-Type	802
81	Tunnel-Private-Group	VLANID (1 to 4095 in hexadecimal)

Note: The specific configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS server software.

When VLAN filtering is enabled, the access point must also have 802.1x authentication enabled and a RADIUS server configured. Wireless clients must also support 802.1x client software to be assigned to a specific VLAN.

When VLAN filtering is disabled, the access point ignores the VLAN tags on any received frames.

Local Bridge Filter – Controls wireless-to-wireless communications between clients through the SMC2552W-G. However, it does not affect communications between wireless clients and the wired network.

- Disable: Allows wireless-to-wireless communications between clients through the access point.
- Enable: Blocks wireless-to-wireless communications between clients through the access point.

AP Management Filter – Controls management access to the SMC2552W-G from wireless clients. Management interfaces include the web, Telnet, or SNMP.

- Disable: Allows management access from wireless clients.
- Enable: Blocks management access from wireless clients.

Ethernet Type Filter – Controls checks on the Ethernet type of all incoming and outgoing Ethernet packets against the protocol filtering table.

- Disable: Access point does not filter Ethernet protocol types.
- Enable: Access point filters Ethernet protocol types based on the configuration of protocol types in the filter table. If a protocol has its status set to “ON,” the protocol is filtered from the access point.

CLI Commands for VLAN Support – From the global configuration mode use the **native-vlanid** command to set the default VLAN ID for the Ethernet interface, then enable VLANs using the **vlan enable** command. When you change the access point's VLAN support setting, you must reboot the access point to implement the change. To view the current VLAN settings, use the **show system** command.

```
SMC-AP(config)#native-vlanid 3                          6-100
SMC-AP(config)#vlan enable                               6-99
Reboot system now? <y/n>: y
SMC-AP#show system                                       6-33

System Information
================================================
Serial Number       : A324003220
System Up time      : 0 days, 0 hours, 32 minutes, 51
seconds
System Name         : r&d
System Location     :
System Contact      : Contact
System Country Code : US - UNITED STATES
MAC Address         : 00-30-F1-91-91-5B
IP Address          : 192.168.2.2
Subnet Mask         : 255.255.255.0
Default Gateway     : 192.168.2.250
VLAN State          : DISABLED
Native VLAN ID      : 3
IAPP State          : ENABLED
DHCP Client         : ENABLED
HTTP Server         : ENABLED
HTTP Server Port    : 80
Slot Status         : Band(g)
Software Version    : v2.0.22
================================================

SMC-AP#
```

CLI Commands for Bridge Filtering – Use the **filter local-bridge** command from the global configuration mode to prevent wireless-to-wireless communications through the access point. Use the **filter ap-manage** command to restrict management access from wireless clients. To configure Ethernet protocol filtering, use the **filter ethernet-type enable** command to enable filtering and the **filter ethernet-type protocol** command to define the protocols that you want to filter. To remove an entry from the table, use the **address filter delete** command. To display the current settings, use the **show filters** command from the Exec mode.

```
SMC-AP(config)#filter local-bridge                        6-60
SMC-AP(config)#filter ap-manage                           6-61
SMC-AP(config)#filter ethernet-type enable                6-62
SMC-AP(config)#filter ethernet-type protocol ARP          6-63
SMC-AP(config)#exit
SMC-AP#show filters                                       6-64

Protocol Filter Information
============================================================
Local Bridge          :ENABLED
AP Management         :ENABLED
Ethernet Type Filter :ENABLED

Enabled Protocol Filters
------------------------------------------------------------
Protocol: ARP                                 ISO: 0x0806
============================================================
SMC-AP#
```

SNMP

You can use a network management application such as SMC's EliteView to manage the SMC2552W-G via the Simple Network Management Protocol (SNMP) from a network management station. To implement SNMP management, the SMC2552W-G must have an IP address and subnet mask, configured either manually or dynamically. Once an IP address has been configured, appropriate SNMP communities and trap receivers should be configured.

Community names are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the access point. To communicate with the access point, a management station must first submit a valid community name for authentication. You therefore need to assign community names to specified users or user groups and set the access level.

SNMP – Enables or disables SNMP management access and also enables the access point to send SNMP traps (notifications). SNMP management is enabled by default.

Location – A text string that describes the system location. (Maximum length: 20 characters)

Contact – A text string that describes the system contact. (Maximum length: 255 characters)

Community Name (Read Only) – Defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects. (Maximum length: 23 characters, case sensitive)

Community Name (Read/Write) – Defines the SNMP community access string that has read/write access. Authorized management stations are able to both retrieve and modify MIB objects. (Maximum length: 23 characters, case sensitive)

Trap Destination IP Address – Specifies the recipient of SNMP notifications. Enter the IP address or the host name. (Host Name: 1 to 20 characters)

Trap Destination Community Name – The community string sent with the notification operation. (Maximum length: 23 characters)

CLI Commands for SNMP – Use the **snmp-server enable server** command from the global configuration mode. To set read/write and read-only community names, use the **snmp-server community** command. Use the **snmp-server location** and **snmp-server contact** commands to indicate the physical location of the access point and define a system contact. The **snmp-server host** command defines a trap receiver host. To view the current SNMP settings, use the **show snmp** command.

```
SMC-AP(config)#snmp-server enable server                6-37
SMC-AP(config)#snmp-server community alpha rw           6-35
SMC-AP(config)#snmp-server community beta ro
SMC-AP(config)#snmp-server location WC-19               6-39
SMC-AP(config)#snmp-server contact Paul                 6-36
SMC-AP(config)#snmp-server host 10.1.19.23 alpha        6-38
SMC-AP(config)#exit
SMC-AP#show snmp                                        6-40

SNMP Information
=========================================
Service State  : Enable
Community (ro) : ****
Community (rw) : *****
Location       : WC-19
Contact        : Paul
Traps          : Enabled
Host Name/IP   : 10.1.19.23
Trap Community : *****
=========================================

SMC-AP#
```

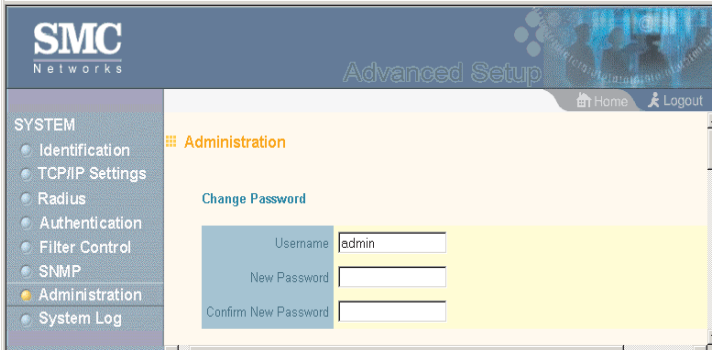
Administration

Changing the Password

Management access to the web and CLI interface on the SMC2552W-G is controlled through a single user name and password. You can also gain additional access security by using control filters (see “Filter Control” on page 5-20).

To protect access to the management interface, you need to configure an Administrator’s user name and password as soon as possible. If the user name and password are not configured, then anyone having access to the access point may be able to compromise access point and network security.

Note: Pressing the Reset button on the back of the SMC2552W-G for more than five seconds resets the user name and password to the factory defaults. For this reason, we recommend that you protect the access point from physical access by unauthorized persons.



Username – The name of the user. The default name is “admin.” (Length: 3-16 characters, case sensitive.)

New Password – The password for management access. (Length: 3-16 characters, case sensitive)

Confirm New Password – Enter the password again for verification.

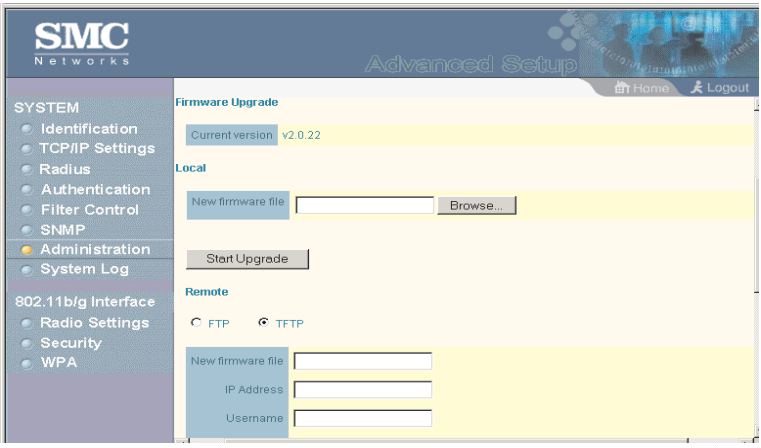
CLI Commands for the User Name and Password – Use the **username** and **password** commands from the CLI configuration mode.

```
SMC-AP(config)#username bob                                    6-21
SMC-AP(config)#password smcadmin                               6-22
SMC-AP#
```

Upgrading Firmware

You can upgrade new SMC2552W-G software from a local file on the management workstation, or from an FTP or TFTP server. New software may be provided periodically on SMC's web site (http://www.smc.com).

After upgrading new software, you must reboot the SMC2552W-G to implement the new code. Until a reboot occurs, the SMC2552W-G will continue to run the software it was using before the upgrade started. Also note that rebooting the access point with new software will reset the configuration to the factory default settings.



Before upgrading new software, verify that the SMC2552W-G is connected to the network and has been configured with a compatible IP address and subnet mask.

If you need to download from an FTP or TFTP server, take the following additional steps:

- Obtain the IP address of the FTP or TFTP server where the access point software is stored.
- If upgrading from an FTP server, be sure that you have an account configured on the server with a user name and password.
- If VLANs are configured on the access point, determine the VLAN ID with which the FTP or TFTP server is associated, and then configure the management station with the same VLAN ID. If you are managing the access point from a wireless client, the VLAN ID for the the wireless client must be configured on a RADIUS server.

Current version – Version number of runtime code.

Firmware Upgrade Local – Downloads an operation code image file from the web management station to the access point using HTTP. Use the Browse button to locate the image file locally on the management station and click Start Upgrade to proceed.

- New firmware file: Specifies the name of the code file on the server. The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

- *Firmware Upgrade Remote* – Downloads an operation code image file from a specified remote FTP or TFTP server. After filling in the following fields, click Start Upgrade to proceed.

- New firmware file: Specifies the name of the code file on the server. The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP

server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

- IP Address: IP address or host name of FTP or TFTP server.
- Username: The user ID used for login on an FTP server.
- Password: The password used for login on an FTP server.

Restore Factory Settings – Click the Restore button to reset the configuration settings for the SMC2552W-G to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to re-enter the default user name (admin) and password (smcadmin) to re-gain management access to this device.

Reset Access Point – Click the Reset button to reboot the system.

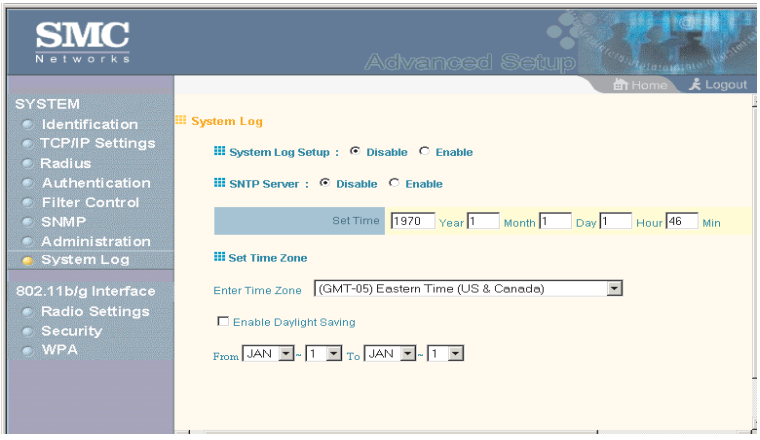
Note: If you have upgraded system software, then you must reboot the SMC2552W-G to implement the new operation code. Before rebooting please reset the access point to the factory default and clear the browser cache.

CLI Commands for Downloading Software from a TFTP Server – Use the **copy tftp file** command from the Exec mode and then specify the file type, name, and IP address of the TFTP server. When the download is complete, the **dir** command can be used to check that the new file is present in the access point file system. To run the new software, use the **reset board** command to reboot the access point.

```
SMC-AP#copy tftp file                                          6-42
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>:  [1]:1
TFTP Source file name:smc-img.bin
TFTP Server IP:192.168.1.19

SMC-AP#dir                                                     6-44
File Name                      Type   File Size
-------------------------     ----  -----------
dflt-img.bin                     2     1319939
smc-img.bin                      2     1629577
syscfg                           5       17776
syscfg_bak                       5       17776

      262144 byte(s) available

SMC-AP#reset board                                             6-14
Reboot system now? <y/n>: y
```

System Log

The SMC2552W-G can be configured to send event and error messages to a System Log Server. The system clock can also be synchronized with a time server, so that all the messages sent to the Syslog server are stamped with the correct time and date.



Enabling System Logging

The SMC2552W-G supports a logging process that can control error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating access point and network problems.

System Log Setup – Enables the logging of error messages.

Logging Host – Enables the sending of log messages to a Syslog server host.

Server Name/IP – The IP address or name of a Syslog server.

Logging Console – Enables the logging of error messages to the console.

Logging Level – Sets the minimum severity level for event logging.

The system allows you to limit the messages that are logged by specifying a minimum severity level. The following table lists the error message levels from the most severe (Alert) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Alert level.

Error Level	**Description**
Alerts	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

Note: The access point error log can be viewed using the Event Logs window in the Status section (page 5-66).The Event Logs window displays the last 128 messages logged in chronological order, from the newest to the oldest. Log messages saved in the access point's memory are erased when the device is rebooted.

CLI Commands for System Logging – To enable logging on the access point, use the **logging on** command from the global configuration mode. The **logging level** command sets the minimum level of message to log. Use the **logging console** command to enable logging to the console. Use the **logging host** command to specify up to four Syslog servers. The CLI also allows the **logging facility-type** command to set the facility-type number to use on the Syslog server. To view the current logging settings, use the **show logging** command.

```
SMC-AP(config)#logging on                                    6-24
SMC-AP(config)#logging level alert                           6-26
SMC-AP(config)#logging console                               6-25
SMC-AP(config)#logging host 1 10.1.0.3 514                   6-24
SMC-AP(config)#logging facility-type 19                      6-27
SMC-AP(config)#exit
SMC-AP#show logging                                          6-27

Logging Information
==========================================
Syslog State                : Enabled
Logging Host State          : Enabled
Logging Console State       : Enabled
Server Domain name/IP       : 1 10.1.0.3
Logging Level               : Error
Logging Facility Type       : 16
==========================================

SMC-AP#
```

Configuring SNTP

Simple Network Time Protocol (SNTP) allows the SMC2552W-G to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The SMC2552W-G acts as an SNTP client, periodically sending time synchronization requests to specific time servers. You can configure up to two time server IP addresses. The access point will attempt to poll each server in the configured sequence.

SNTP Server – Configures the access point to operate as an SNTP client. When enabled, at least one time server IP address must be specified.

- Primary Server: The IP address of an SNTP or NTP time server that the access point attempts to poll for a time update.
- Secondary Server: The IP address of a secondary SNTP or NTP time server. The access point first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server.

Note: The SMC2552W-G also allows you to disable SNTP and set the system clock manually.

Set Time Zone – SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours your time zone is located before (east) or after (west) UTC.

Enable Daylight Saving – The access point provides a way to automatically adjust the system clock for Daylight Savings Time

changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour.

CLI Commands for SNTP – To enable SNTP support on the access point, from the global configuration mode specify SNTP server IP addresses using the **sntp-server ip** command, then use the **sntp-server enable** command to enable the service. Use the **sntp-server timezone** command to set the time zone for your location, and the **sntp-server daylight-saving** command to set daylight savings. To view the current SNTP settings, use the **show sntp** command.

```
SMC-AP(config)#sntp-server ip 10.1.0.19                    6-28
SMC-AP(config)#sntp-server enable                          6-29
SMC-AP(config)#sntp-server timezone +8                     6-32
SMC-AP(config)#sntp-server daylight-saving                 6-31
Enter Daylight saving from which month<1-12>: 3
and which day<1-31>: 31
Enter Daylight saving end to which month<1-12>: 10
and which day<1-31>: 31
SMC-AP(config)#exit
SMC-AP#show sntp                                           6-32

SNTP Information
============================================================
Service State        : Enabled
SNTP (server 1) IP   : 137.92.140.80
SNTP (server 2) IP   : 192.43.244.18
Current Time         : 19 : 35, Jan 10th, 2004
Time Zone            : +8 (TAIPEI, BEIJING)
Daylight Saving      : Enabled, from Mar, 31th to Oct,
31th
============================================================

SMC-AP#
```

CLI Commands for the System Clock – The following example shows how to manually set the system time when SNTP server support is disabled on the access point.

```
SMC-AP(config)#no sntp-server enable                    6-29
SMC-AP(config)#sntp-server date-time                    6-30
Enter Year<1970-2100>: 2004
Enter Month<1-12>: 10
Enter Day<1-31>: 10
Enter Hour<0-23>: 18
Enter Min<0-59>: 35
SMC-AP(config)#
```

Radio Interface

The IEEE 802.11b and 802.11g interface includes configuration options for radio signal characteristics and wireless security features.

The access point can operate in three modes, IEEE 802.11b only, 802.11g only, or a mixed 802.11b/g mode. Also note that 802.11g is backward compatible with 802.11b. The 802.11b/g interface can be configured independently under the following web pages:

- Radio Interface : 802.11b/g

Note: The radio channel settings for the SMC2552W-G are limited by local regulations, which determine the number of channels that are available.

Radio Settings (802.11g)

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Also note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

Enable – Enables radio communications on the SMC2552W-G. (Default: Enabled)

Radio Channel – The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least four channels apart to avoid interference with each other. For example, in the United States you can deploy up to four access points in the same area (e.g., channels 1, 6, 11). Also note that the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked. (Range: 1-11; Default: 1)

Auto Channel Select – Enables the access point to automatically select an unoccupied radio channel. (Default: Enabled)

SSID Broadcast – The SSID broadcast can be disabled to prevent access to clients without a pre-configured SSID. When disabled, the access point will not include its SSID in beacon messages. Nor will it respond to probe requests from clients that do not include the correct SSID. (Default: Enabled)

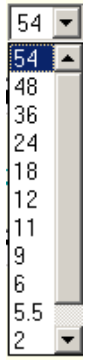
Select Antenna Mode – Specifies whether the antenna used will be automatically selected based on best signal reception (i.e., Diversity mode), or will be fixed to use an optional high-gain antenna. (Default: Diversity)

Working Mode – The access point can be configured to support both 802.11b and 802.11g clients simultaneously, 802.11b clients only, or 802.11g clients only. (Default: 802.11b and 802.11g)

Transmit Power – Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not

interfere with the operation of other radio devices in the service area. (Options: 100%, 50%, 25%, 12%, minimum; Default: 100%)

Maximum Station Data Rate – The maximum data rate at which a client can connect to the access point. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Options: 54, 48, 36, 24 Mbps; Default: 54 Mbps)



Beacon Interval – The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)

Data Beacon Rate – The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 2 beacons)

RTS Threshold – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the

sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the access point never sends RTS signals. If set to 2347, the access point always sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes: Default: 2347 bytes)

CLI Commands for the 802.11g Wireless Interface – From the global configuration mode, enter the **interface wireless g** command to access the 802.11g radio interface. Set the interface SSID using the **ssid** command and, if required, configure a name for the interface using the **description** command. You can also use the **no ssid-broadcast** command to stop sending the SSID in beacon messages. Select a radio channel or set selection to Auto using the **channel** command. Set any other parameters as required. To view the current 802.11g radio settings, use the **show interface wireless g** command.

```
SMC-AP(config)#interface wireless g                              6-68
Enter Wireless configuration commands, one per line.
SMC-AP(if-wireless g)#description RD-AP#3                        6-75
SMC-AP(if-wireless g)#ssid r&d                                   6-78
SMC-AP(if-wireless g)#channel auto                               6-77
SMC-AP(if-wireless g)#ssid-broadcast                             6-75
SMC-AP(if-wireless g)#select-antenna-mode right antenna          6-74
SMC-AP(if-wireless g)#radio-mode g                               6-73
SMC-AP(if-wireless g)#transmit-power full                        6-86
SMC-AP(if-wireless g)#speed 6                                    6-76
SMC-AP(if-wireless g)#max-association 32                         6-87
SMC-AP(if-wireless g)#beacon-interval 150                        6-78
SMC-AP(if-wireless g)#dtim-period 5                              6-79
SMC-AP(if-wireless g)#fragmentation-length 512                   6-80
SMC-AP(if-wireless g)#rts-threshold 256                          6-81
SMC-AP(if-wireless g)#exit
```

```
SMC-AP#show interface wireless g                                    6-95

Wireless Interface Information
============================================================
---------------Identification-----------------------------
Description                : Enterprise 802.11g Access Point
SSID                       : r&d
Channel                    : 11 (AUTO)
Status                     : Enable
----------------802.11 Parameters-------------------------
Transmit Power             : HALF (10 dBm)
Max Station Data Rate      : 6Mbps
Fragmentation Threshold    : 512 bytes
RTS Threshold              : 256 bytes
Beacon Interval            : 150 TUs
DTIM Interval              : 5 beacons
Maximum Association        : 32 stations
----------------Security-----------------------------------
SSID Broadcast             : ENABLED
Multicast cipher           : WEP
Unicast cipher             : WEP
WPA clients                : SUPPORTED
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
   Key 1: EMPTY   Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type        : OPEN
============================================================
SMC-AP#
```

Security

The SMC2552W-G is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

To improve wireless network security, you have to implement two main functions:

- Authentication: It must be verified that clients attempting to connect to the network are authorized users.
- Traffic Encryption: Data passing between the access point and clients must be protected from interception and evesdropping.

For a more secure network, the access point can implement one or a combination of the following security mechanisms:

- Wired Equivalent Privacy (WEP) page 5-49
- IEEE 802.1x page 5-14
- Wireless MAC address filtering page 5-13
- Wi-Fi Protected Access (WPA) page 5-54

The security mechanisms that may be employed depend on the level of security required, the network and management resources available, and the software support provided on wireless clients. A summary of wireless security considerations is listed in the following table.

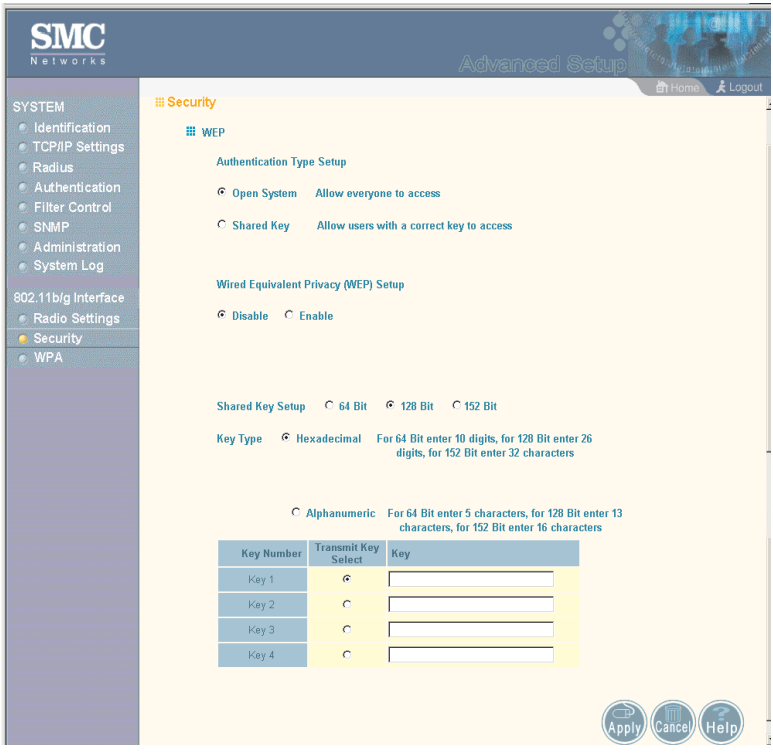
Security Mechanism	Client Support	Implementation Considerations
WEP	Built-in support on all 802.11b and 802.11g devices	• Provides only weak security • Requires manual key management
WEP with 802.1x	Requires 802.1x client support in system or by add-in software (native support provided in Windows XP)	• Provides dynamic key rotation for improved WEP security • Requires configured RADIUS server • 802.1x EAP type may require management of digital certificates for clients and server
MAC Address Filtering	Uses the MAC address of client network card	• Provides only weak user authentication • Management of authorized MAC addresses • Can be combined with other methods for improved security • Optionally configured RADIUS server
WPA Enterprise Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides robust security in WPA-only mode • Offers support for legacy WEP clients, but with increased security risk • Requires configured RADIUS server • 802.1x EAP type may require management of digital certificates for clients and server
WPA PSK Mode	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides good security in small networks • Requires manual management of pre-shared key

Note: Although a WEP static key is not needed for WEP over 802.1x, WPA over 802.1x, and WPA PSK modes, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point.

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be flawed. For more robust wireless security, the SMC2552W-G provides Wi-Fi Protected Access (WPA) for improved data encryption and user authentication.



Setting up shared keys enables the basic IEEE 802.11 Wired Equivalent Privacy (WEP) on the access point to prevent unauthorized access to the network.

If you choose to use WEP shared keys instead of an open system, be sure to define at least one static WEP key for user authentication and data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Authentication Type Setup – Sets the access point to communicate as an open system that accepts network access attempts from any client, or with clients using pre-configured static shared keys.

- Open System: Select this option if you plan to use WPA or 802.1x as a security mechanism. If you don't set up any other security mechanism on the access point, the network has no protection and is open to all users. This is the default setting.
- Shared Key: Sets the access point to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.

Note: To use 802.1x on wireless clients requires a network card driver and 802.1x client software that supports the EAP authentication type that you want to use. Windows XP provides native WPA support, other systems require additional software.

Wired Equivalent Privacy (WEP) Setup – Enable or disable the access point to use WEP shared keys for data encryption. If this option is selected, you must configure at least one key on the access point and all clients. (Default: Disable)

Note: Although WEP keys are not needed for WPA, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point.

Shared Key Setup – Select 64 Bit, 128 Bit, or 152 Bit key length. Note that the same size of encryption key must be supported on all wireless clients. (Default: 128 Bit)

Key Type – Select the preferred method of entering WEP encryption keys on the access point and enter up to four keys:

- Hexadecimal: Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys.
- Alphanumeric: Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys, or 16 alphanumeric characters for 152 bit keys.
- Transmit Key Select: Selects the key number to use for encryption. If the clients have all four keys configured to the same values, you can change the encryption key to any of the four settings without having to update the client keys.

Note: Key index and type must match that configured on the clients.

The configuration settings for WEP are summarized below:

WEP only	**WEP over 802.1x**
Authentication Type: Shared Key WEP (encryption): Enable WPA clients only: Disable Multicast Cipher: WEP Shared Key: 64/128/152 Key Type - Hex: 10/26/32 characters ASCII: 5/13/16 characters Transmit Key: 1/2/3/4 (set index) 802.1x = Disabled[1] MAC Authentication: Any setting[2]	Authentication Type: Open System WEP (encryption): Enable WPA clients only: Disable Multicast Cipher: WEP Shared Key: 64/128 802.1x = Required[1] MAC Authentication: Disabled/Local[2]

1: See Authentication (page 5-12)
2: See Radius (page 5-9)

CLI Commands for WEP Shared Key Security – From the 802.11g interface configuration mode, use the **authentication** command to enable WEP shared-key authentication and the **encryption** command to enable WEP encryption. Use the **multicast-cipher** command to select WEP cipher type. To enter WEP keys, use the **key** command, and then set one key as the transmit key using the **transmit-key** command. Then disable 802.1x port authentication with the **802.1x** command. To view the current security settings, use the **show interface wireless g** command.

```
SMC-AP(config)#interface wireless g                          6-68
Enter Wireless configuration commands, one per line.
SMC-AP(if-wireless g)#authentication shared                  6-82
SMC-AP(if-wireless g)#encryption 128                         6-83
SMC-AP(if-wireless g)#multicast-cipher wep                   6-88
SMC-AP(if-wireless g)#key 1 128 ascii abcdeabcdeabc          6-84
SMC-AP(if-wireless g)#transmit-key 1                         6-85
SMC-AP(if-wireless g)#end
SMC-AP(config)#no 802.1x                                     6-51
SMC-AP(config)#end
SMC-AP#show interface wireless g                             6-95

Wireless Interface 802.11g Information
============================================================
---------------Identification-----------------------------
Description                : Enterprise 802.11g Access Point
SSID                       : r&d
Channel                    : 11 (AUTO)
Status                     : Enable
----------------802.11 Parameters-------------------------
Transmit Power             : HALF (10 dBm)
Max Station Data Rate      : 54Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
DTIM Interval              : 2 beacons
Maximum Association        : 32 stations
```

```
----------------Security----------------------------------
SSID Broadcast              : DISABLED
Multicast cipher            : TKIP
Unicast cipher              : WEP
WPA clients                 : SUPPORTED
Encryption                  : 128-BIT ENCRYPTION
Default Transmit Key        : 1
Static Keys :
   Key 1: *****     Key 2: EMPTY     Key 3: EMPTY     Key 4: EMPTY
Authentication Type         : SHARED
============================================================
SMC-AP#
```

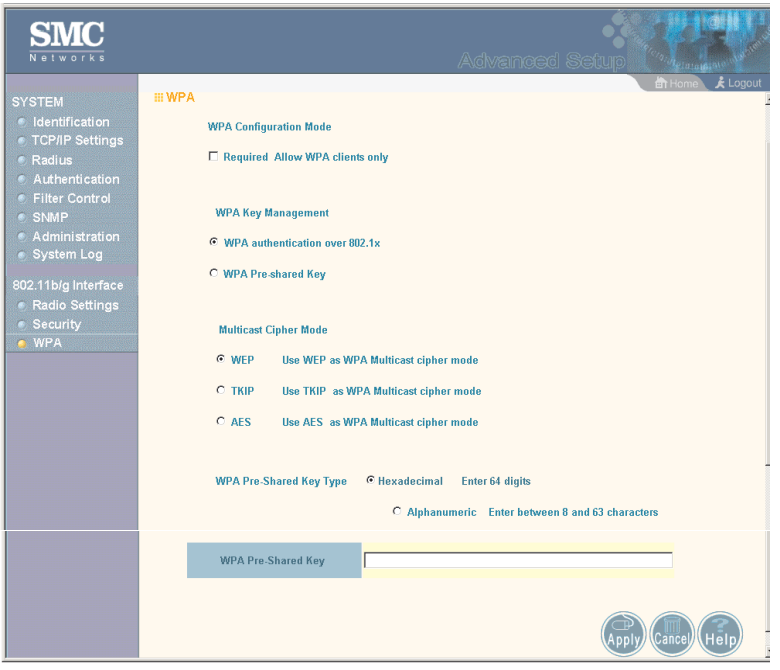
Note: The index and length values used in the **key** command must be the same values used in the **encryption** and **transmit-key** commands.

CLI Commands for WEP over 802.1x Security – From the 802.11g interface configuration mode, use the **authentication** command to select open system authentication. Use the **multicast-cipher** command to select WEP cipher type. Then set 802.1x to required with **802.1x** command, and disable MAC authentication with the **mac-authentication** command. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
SMC-AP(config)#interface wireless g                    6-68
Enter Wireless configuration commands, one per line.
SMC-AP(if-wireless g)#authentication open              6-82
SMC-AP(if-wireless g)#encryption 128                   6-83
SMC-AP(if-wireless g)#multicast-cipher wep             6-88
SMC-AP(if-wireless g)#end
SMC-AP(config)#802.1x required                         6-51
SMC-AP(config)#no mac-authentication                   6-57
SMC-AP(config)#
```

Wi-Fi Protected Access (WPA)

WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks.



The SMC2552W-G supports the following WPA components and features:

IEEE 802.1x and the Extensible Authentication Protocol (EAP): WPA employs 802.1x as its basic framework for user authentication and dynamic key management. The 802.1x client and RADIUS server should use an appropriate EAP type—such as EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS), or PEAP (Protected EAP)—for strongest authentication. Working together, these protocols provide “mutual authentication” between a client, the access point, and a RADIUS server that

prevents users from accidentally joining a rogue network. Only when a RADIUS server has authenticated a user's credentials will encryption keys be sent to the access point and client.

Note: To implement WPA on wireless clients requires a WPA-enabled network card driver and 802.1x client software that supports the EAP authentication type that you want to use. Windows XP provides native WPA support, other systems require additional software.

Temporal Key Integrity Protocol (TKIP): WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. Basically, TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet. TKIP provides further data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.

WPA Pre-Shared Key (**PSK**) **Mode**: For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

Mixed WPA and WEP Client Support: WPA enables the access point to indicate its supported encryption and authentication mechanisms to clients using its beacon signal. WPA-compatible clients can likewise respond to indicate their WPA support. This enables the access point to determine which clients are using

WPA security and which are using legacy WEP. The access point uses TKIP unicast data encryption keys for WPA clients and WEP unicast keys for WEP clients. The global encryption key for multicast and broadcast traffic must be the same for all clients, therefore it restricts encryption to a WEP key.

When access is opened to both WPA and WEP clients, no authentication is provided for the WEP clients through shared keys. To support authentication for WEP clients in this mixed mode configuration, you can use either MAC authentication or 802.1x authentication.

Advanced Encryption Standard (**AES**) **Support**: WPA specifies AES encryption as an optional alternative to TKIP and WEP. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP. The developing IEEE 802.11i wireless security standard has specified AES as an eventual replacement for TKIP and WEP. However, because of the difference in ciphering algorithms, AES requires new hardware support in client network cards that is currently not widely available. The access point includes AES support as a future security enhancement.

The WPA configuration parameters are described below:

WPA Configuration Mode – The access point can be configured to allow only WPA-enabled clients to access the network, or also allow clients only capable of supporting WEP.

WPA Key Management – WPA can be configured to work in an enterprise environment using IEEE 802.1x and a RADIUS server for user authentication. For smaller networks, WPA can be enabled using a common pre-shared key for client authentication with the access point.

- WPA authentication over 802.1x: The WPA enterprise mode that uses IEEE 802.1x to authenticate users and to dynamically distribute encryption keys to clients.
- WPA Pre-shared Key: The WPA mode for small networks that uses a common password string that is manually distributed. If this mode is selected, be sure to also specify the key string.

Multicast Cipher Mode – Selects an encryption method for the global key used for multicast and broadcast traffic, which is supported by all wireless clients.

- WEP: WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly-sensitive data.
- TKIP: TKIP provides data encryption enhancements including per-packet key hashing (that is, changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
- AES: AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.

WPA Pre-Shared Key Type – If the WPA pre-shared-key mode is used, all wireless clients must be configured with the same key to communicate with the access point.

- Hexadecimal: Enter a key as a string of 64 hexadecimal numbers.
- Alphanumeric: Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters, which can include spaces.

The configuration settings for WPA are summarized below:

WPA pre-shared key only	**WPA over 802.1x**
Authentication Type: Open System WEP (encryption): Enable[1] WPA clients only: Enable WPA Mode: Pre-shared-key Multicast Cipher: WEP/TKIP/AES[2] WPA PSK Type - Hex: 64 characters ASCII: 8-63 characters Shared Key: 64/128/152 802.1x = Disabled[3] MAC Authentication: Disabled/Local[4]	Authentication Type: Open System WEP (encryption): Enable[1] WPA clients only: Enable WPA Mode: WPA over 802.1x Multicast Cipher: WEP/TKIP/AES[2] Shared Key: 64/128/152 802.1x = Required[3] MAC Authentication: Disabled/Local[4]

1: Although WEP keys are not needed for WPA, you must enable WEP encryption through the web or CLI in order to enable all types of encryption in the access point. For example, use the CLI **encryption** command to set Encryption = 64, 128 or 152, thus enabling encryption (i.e., all types of encryption) in the access point.
2: Do not use WEP unless the access point must support both WPA and WEP clients.
3: See Authentication (page 5-12)
4: See Radius (page 5-9)

CLI Commands for WPA Pre-shared Key Security – From the 802.11g interface configuration mode, use the **authentication** command to set the access point to "Open System." Use the WEP **encryption** command to enable all types of encryption. To enable WPA to be required for all clients, use the **wpa-clients** command. Use the **wpa-mode** command to enable the Pre-shared Key mode. To enter a key value, use the **wpa-psk-type** command to specify a hexadecimal or alphanumeric key, and then use the **wpa-preshared-key** command to define the key. Then disable 802.1x and MAC authentication. To view the current 802.11g security settings, use

the **show interface wireless g** command (not shown in example).

```
SMC-AP(config)#interface wireless g                    6-68
Enter Wireless configuration commands, one per line.
SMC-AP(if-wireless g)#authentication open              6-82
SMC-AP(if-wireless g)#encryption 128                   6-83
SMC-AP(if-wireless g)#wpa-clients required             6-89
SMC-AP(if-wireless g)#wpa-mode pre-shared-key          6-91
SMC-AP(if-wireless g)#wpa-psk-type alphanumeric        6-93
SMC-AP(if-wireless g)#wpa-preshared-key ASCII asecret  6-92
SMC-AP(if-wireless g)#end
SMC-AP(config)#no 802.1x                               6-51
SMC-AP(config)#no mac-authentication                   6-57
```

CLI Commands for WPA over 802.1x Security – From the 802.11g interface configuration mode, use the **authentication** command to set the access point to "Open System." Use the WEP **encryption** command to enable all types of encryption. Use the **wpa-clients** command to set WPA to be required or supported for clients. Use the **wpa-mode** command to enable WPA dynamic keys over 802.1x. Set the broadcast and multicast key encryption using the **multicast-cipher** command. Then set 802.1x to required, and disable MAC authentication. To view the current 802.11g security settings, use the **show interface wireless g** command (not shown in example).

```
SMC-AP(config)#interface wireless g                    6-68
Enter Wireless configuration commands, one per line.
SMC-AP(if-wireless g)#authentication open              6-82
SMC-AP(if-wireless g)#encryption 128                   6-83
SMC-AP(if-wireless g)#wpa-clients required             6-89
SMC-AP(if-wireless g)#wpa-mode dynamic                 6-91
SMC-AP(if-wireless g)#multicast-cipher TKIP            6-88
SMC-AP(if-wireless g)#end
SMC-AP(config)#802.required                            6-51
SMC-AP(config)#no mac-authentication                   6-57
```

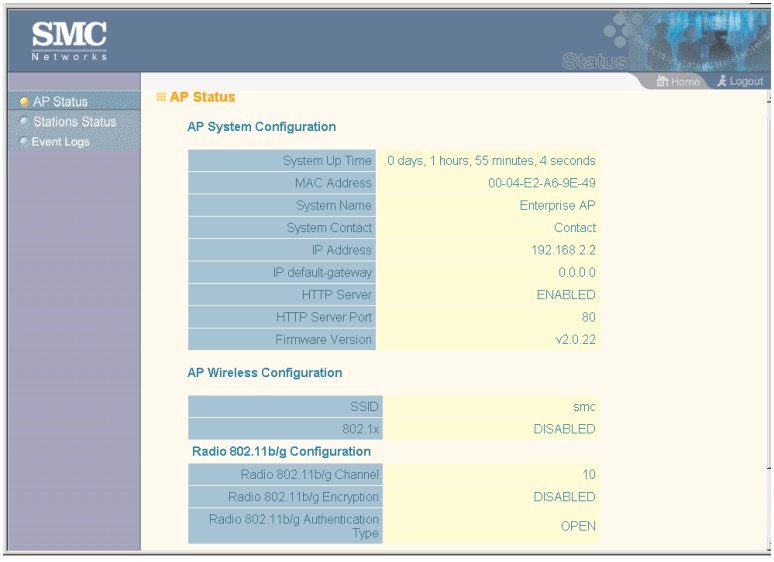
Status Information

The Status page includes information on the following items:

Menu	Description	Page
AP Status	Displays configuration settings for the basic system and the wireless interface	5-61
Station Status	Shows the wireless clients currently associated with the access point	5-64
Event Logs	Shows log messages stored in memory	5-66

Access Point Status

The AP Status window displays basic system configuration settings, as well as the settings for the wireless interface.



AP System Configuration – The AP System Configuration table displays the basic system configuration settings:

- System Up Time: Length of time the management agent has been up.
- MAC Address: The physical layer address for this device.
- System Name: Name assigned to this system.
- System Contact: Administrator responsible for the system.
- IP Address: IP address of the management interface for this device.
- IP Default Gateway: IP address of the gateway router between this device and management stations that exist on other network segments.
- HTTP Server: Shows if management access via HTTP is enabled.
- HTTP Server Port: Shows the TCP port used by the HTTP interface.
- Version: Shows the version number for the runtime code.

AP Wireless Configuration – The AP Wireless Configuration table displays the 802.11b/g wireless interface settings listed below.

- SSID: The service set identifier for this wireless group.
- Radio Channel: The radio channel through which the access point communicates with wireless clients.
- Radio Encryption: The key size used for data encryption.
- Radio Authentication Type: Shows if open system or shared key authentication is used.
- 802.1x: Shows if IEEE 802.1x access control for wireless clients is enabled.

CLI Commands for Displaying System Settings – To view the current access point system settings, use the **show system** command from the Exec mode. To view the current radio interface settings, use the **show interface wireless g** command (see page 6-95).

```
SMC-AP#show system                                          6-33
System Information
============================================================
Serial Number        : A324003220
System Up time       : 0 days, 4 hours, 39 minutes, 46
seconds
System Name          : Enterprise AP
System Location      :
System Contact       : Contact
System Country Code  : US - UNITED STATES
MAC Address          : 00-30-F1-91-91-5B
IP Address           : 192.168.2.2
Subnet Mask          : 255.255.255.0
Default Gateway      : 192.168.2.250
VLAN State           : DISABLED
Native VLAN ID       : 1
IAPP State           : ENABLED
DHCP Client          : ENABLED
HTTP Server          : ENABLED
HTTP Server Port     : 80
Slot Status          : Band(g)
Software Version     : v2.0.22
============================================================
SMC-AP#
```

Station Status

The Station Status window shows the wireless clients currently associated with the SMC2552W-G.

The Station Configuration page displays basic connection information for all associated stations as described below. Note that this page is automatically refreshed every five seconds.

- Station Address: The MAC address of the wireless client.
- Authenticated: Shows if the station has been authenticated. The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to stations before attempting authentication.
- Associated: Shows if the station has been successfully associated with the access point. Once authentication is completed, stations can associate with the current access point, or reassociate with a new access point. The association

procedure allows the wireless system to track the location of each mobile client, and ensure that frames destined for each client are forwarded to the appropriate access point.

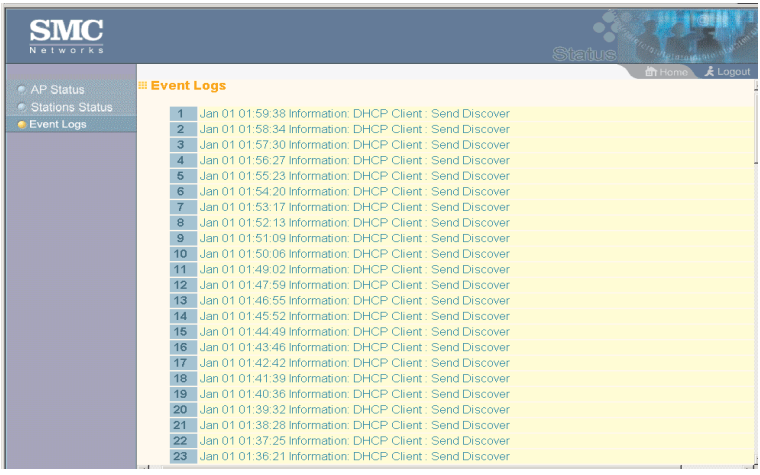
- Forwarding Allowed: Shows if the station has passed 802.1x authentication and is now allowed to forward traffic to the access point.
- Key Type: Displays “Open System” or “Shared Key.”

CLI Commands for Displaying Station Status – To view status of clients currently associated with the access point, use the **show station** command from the Exec mode.

```
SMC-AP#show station                                          6-96

802.11g Station Table
Station Address   : 00-04-E2-41-C2-9D
        Authenticated        : TRUE
        Associated           : TRUE
        Forwarding Allowed   : TRUE
SMC-AP#
```

Event Logs

The Event Logs window shows the log messages generated by the access point and stored in memory.


SMC
Networks
Status
Home
Logout
AP Status
Stations Status
Event Logs
Event Logs
1 Jan 01 01:59:38 Information: DHCP Client : Send Discover
2 Jan 01 01:58:34 Information: DHCP Client : Send Discover
3 Jan 01 01:57:30 Information: DHCP Client : Send Discover
4 Jan 01 01:56:27 Information: DHCP Client : Send Discover
5 Jan 01 01:55:23 Information: DHCP Client : Send Discover
6 Jan 01 01:54:20 Information: DHCP Client : Send Discover
7 Jan 01 01:53:17 Information: DHCP Client : Send Discover
8 Jan 01 01:52:13 Information: DHCP Client : Send Discover
9 Jan 01 01:51:09 Information: DHCP Client : Send Discover
10 Jan 01 01:50:06 Information: DHCP Client : Send Discover
11 Jan 01 01:49:02 Information: DHCP Client : Send Discover
12 Jan 01 01:47:59 Information: DHCP Client : Send Discover
13 Jan 01 01:46:55 Information: DHCP Client : Send Discover
14 Jan 01 01:45:52 Information: DHCP Client : Send Discover
15 Jan 01 01:44:49 Information: DHCP Client : Send Discover
16 Jan 01 01:43:46 Information: DHCP Client : Send Discover
17 Jan 01 01:42:42 Information: DHCP Client : Send Discover
18 Jan 01 01:41:39 Information: DHCP Client : Send Discover
19 Jan 01 01:40:36 Information: DHCP Client : Send Discover
20 Jan 01 01:39:32 Information: DHCP Client : Send Discover
21 Jan 01 01:38:28 Information: DHCP Client : Send Discover
22 Jan 01 01:37:25 Information: DHCP Client : Send Discover
23 Jan 01 01:36:21 Information: DHCP Client : Send Discover

The Event Logs table displays the following information:

- Log Time: The time the log message was generated.
- Event Level: The logging level associated with this message. For a description of the various levels, see “logging level” on page 5-34.
- Event Message: The content of the log message.

Error Messages – An example of a logged error message is:

“Station Failed to authenticate (unsupported algorithm).”

This message may be caused by any of the following conditions:

- Access point was set to “Open Authentication,” but a client sent an authentication request frame with a “Shared key.”
- Access point was set to “Shared Key Authentication,” but a client sent an authentication frame for “Open System.”

- WEP keys do not match: When the access point uses “Shared Key Authentication,” but the key used by client and access point are not the same, the frame will be decrypted incorrectly, using the wrong algorithm and sequence number.

CLI Commands for Displaying the Event Logs – From the global configuration mode, use the **show logging** command.

```
SMC-AP#show logging                                          6-27

Logging Information
==========================================
Syslog State                : Enabled
Logging Host State          : Enabled
Logging Console State       : Enabled
Server Domain name/IP       : 192.168.1.19
Logging Level               : Alert
Logging Facility Type       : 16
==========================================
SMC-AP#
```

Note: Log messages are not displayed in the CLI.

Chapter 6
Command Line Interface

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the SMC2552W-G over a direct connection to the console port, or via a Telnet connection, the access point can be managed by entering command keywords and parameters at the prompt. Using the access point's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the access point through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user name is "admin" and the default password is "smcadmin.") When the user name is entered, the CLI displays the "SMC Enterprise AP#" prompt.
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "exit" command.

After connecting to the system through the console port, the login screen displays:

```
Username: admin
Password: smcadmin
SMC Enterprise AP#
```

Note: Command examples shown later in this chapter abbreviate the console prompt to “SMC-AP” for simplicity.

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, if the access point cannot acquire an IP address from a DHCP server, the default IP address used by the access point, 192.168.2.2, consists of a network portion (192.168.2) and a host portion (2).

To access the access point through a Telnet session, you must first set the IP address for the access point, and set the default gateway if you are managing the access point from a different IP subnet. For example:

```
SMC-AP#configure
SMC-AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
SMC-AP(if-ethernet)#ip address 10.1.0.1 255.255.255.0
 10.1.0.254
SMC-AP(if-ethernet)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the access point with an IP address, you can open a Telnet session by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “SMC Enterprise AP#” prompt to show that you are using executive access mode (i.e., Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password: smcadmin
SMC-AP#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces ethernet,” **show** and **interfaces** are keywords, and **ethernet** is an argument that specifies the interface type.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
SMC Enterprise AP(config)#username smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "configure" example, typing **con** followed by a tab will result in printing the command up to "**configure**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by following a command with the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current configuration mode (Exec, Global Configuration, or Interface). You can also display a

list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
SMC-AP#show ?
  authentication  Show Authentication parameters
  bootfile        Show bootfile name
  filters         Show filters
  hardware        Show hardware version
  history         Display the session history
  interface       Show interface information
  line            TTY line information
  logging         Show the logging buffers
  radius          Show radius server
  snmp            Show snmp statistics
  sntp            Show sntp statistics
  station         Show 802.11 station table
  system          Show system information
  version         Show system version
SMC-AP#show
```

The command "**show interface?**" will display the following information:

```
SMC-AP#show interface ?
  ethernet  Show Ethernet interface
  wireless  Show wireless interface
  <cr>
SMC-AP#show interface
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
SMC-AP#show s?
snmp     sntp     station  system
SMC-AP#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	**Mode**
Exec	Privileged
Configuration	Global
	Interface-ethernet
	Interface-wireless

Exec Commands

When you open a new console session on access point, the system enters Exec command mode. Only a limited number of the commands are available in this mode. You can access all other commands only from the configuration mode. To access Exec mode, open a new console session with the user name "admin." The command prompt displays as "SMC Enterprise AP#" for Exec mode.

```
Username: admin
Password: [system login password]
SMC-AP#
```

Configuration Commands

Configuration commands are used to modify access point settings. These commands modify the running configuration and are saved in memory.

The configuration commands are organized into three different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **username** and **password**.
- Interface-Ethernet Configuration - These commands modify the Ethernet port configuration, and include command such as **dns** and **ip**.
- Interface-Wireless Configuration - These commands modify the wireless port configuration, and include command such as **ssid** and **authentication**.

To enter the Global Configuration mode, enter the command **configure** in Exec mode. The system prompt will change to "SMC Enterprise AP(config)#" which gives you access privilege to all Global Configuration commands.

```
SMC-AP#configure
Enter Ethernet configuration commands, one per line.
SMC-AP(config)#
```

To enter Interface mode, you must enter the "**interface ethernet**," or "**interface wireless g**" command while in Global Configuration mode. The system prompt will change to "SMC Enterprise AP(if-ethernet)#," or SMC Enterprise AP(if-wireless)" indicating that you have access privileges to the associated commands. You can use the **end** command to return to the Exec mode.

```
SMC-AP(config)#interface ethernet
SMC-AP(if-ethernet)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates a task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes from cursor to the end of the command line.
Ctrl-L	Repeats current command line on a new line.

Keystroke	**Function**
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor backward one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
General	Basic commands for entering configuration mode, restarting the system, or quitting the CLI	6-11
System Management	Controls user name, password, system logs, browser management options, clock settings, and a variety of other system information	6-16
SNMP	Configures community access strings and trap managers	6-35
Flash/File	Manages code image or access point configuration files	6-40
RADIUS	Configures the RADIUS client used with 802.1x authentication	6-45
Authentication	Configures IEEE 802.1x port access control and address filtering	6-50
Filtering	Filters communications between wireless clients, controls access to the management interface from wireless clients, and filters traffic using specific Ethernet protocol types	6-60
Interface	Configures connection parameters for the Ethernet port and wireless interface	6-65
IAPP	Enables roaming between multi-vendor access points	6-97
VLANs	Configures VLAN membership	6-98

The access mode shown in the following tables is indicated by these abbreviations: **GC** (Global Configuration), and **IC** (Interface Configuration.

General Commands

Command	Function	Mode	Page
configure	Activates global configuration mode	Exec	6-11
end	Returns to Exec mode	GC, IC	6-12
exit	Returns to the previous configuration mode, or exits the CLI	any	6-12
ping	Sends ICMP echo request packets to another node on the network	Exec	6-13
reset	Restarts the system	Exec	6-14
show history	Shows the command history buffer	Exec	6-14
show line	Shows the configuration settings for the console port	Exec	6-15

configure

This command activates Global Configuration mode. You must enter this mode to modify most of the settings on the access point. You must also enter Global Configuration mode prior to enabling the context modes for Interface Configuration. see “Using the Command Line Interface” on page 6-1

Default Setting

None

Command Mode

Exec

Example

```
SMC-AP#configure
Enter Ethernet configuration commands, one per line.
SMC-AP(config)#
```

Related Commands

end (page 6-12)

end

This command returns to the previous configuration mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration

Example

This example shows how to return to the Configuration mode from the Interface Configuration mode:

```
SMC-AP(if-ethernet)#end
SMC-AP(config)#
```

exit

This command returns to the Exec mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Exec mode from the Interface Configuration mode, and then quit the CLI session:

```
SMC-AP(if-ethernet)#exit
SMC-AP#exit
CLI session with the Access Point is now closed

Username:
```

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping <*host_name* | *ip_address*>

- *host_name* - Alias of the host.
- *ip_address* - IP address of the host.

Default Setting

None

Command Mode

Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
SMC-AP#ping 192.168.2.2
192.168.2.2 is alive
SMC-AP#
```

reset

This command restarts the system or restores the factory default settings.

Syntax

reset <**board** | **configuration**>

- **board** - Reboots the system.
- **configuration** - Resets the configuration settings to the factory defaults, and then reboots the system.

Default Setting

None

Command Mode

Exec

Command Usage

When the system is restarted, it will always run the Power-On Self-Test.

Example

This example shows how to reset the system:

```
SMC-AP#reset board
Reboot system now? <y/n>: y
```

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Exec

Command Usage

- The history buffer size is fixed at 10 commands.
- Use the up or down arrow keys to scroll through the commands in the history buffer.

Example

In this example, the show history command lists the contents of the command history buffer:

```
SMC-AP#show history
 config
 exit
 show history
SMC-AP#
```

show line

This command displays the console port's configuration settings.

Command Mode

Exec

Example

The console port settings are fixed at the values shown below.

```
SMC-AP#show line
Console Line Information
=======================================================
  databits   : 8
  parity     : none
  speed      : 9600
  stop bits  : 1
=======================================================
SMC-AP#
```

System Management Commands

These commands are used to configure the user name, password, system logs, browser management options, clock settings, and a variety of other system information.

Command	Function	Mode	Page
Country Setting	Sets the country code for correct radio operation		
country	Sets the access point country code	Exec	6-18
Device Designation	Configures information that uniquely identifies this device		
prompt	Customizes the command line prompt	GC	6-20
system name	Specifies the host name for the access point	GC	6-20
snmp-server contact	Sets the system contact string	GC	6-36
snmp-server location	Sets the system location string	GC	6-39
User Access	Configures the user name and password for management access		
username	Configures the user name for management access	GC	6-21
password	Specifies the password for management access	GC	6-22
Web Server	Enables management access via a web browser		
ip http port	Specifies the port to be used by the web browser interface	GC	6-22
ip http server	Allows the access point to be monitored or configured from a browser	GC	6-23
Event Logging	Controls logging of error messages		
logging on	Controls logging of error messages	GC	6-24
logging host	Adds a syslog server host IP address that will receive logging messages	GC	6-24

Command	Function	Mode	Page
logging console	Initiates logging of error messages to the console	GC	6-25
logging level	Defines the minimum severity level for event logging	GC	6-26
logging facility-type	Sets the facility type for remote logging of syslog messages	GC	6-27
show logging	Displays the state of logging	Exec	6-27
System Clock	Sets the system clock via an NTP/ SNTP server		
sntp-server ip	Specifies one or more time servers	GC	6-28
sntp-server enable	Accepts time from the specified time servers	GC	6-29
sntp-server date-time	Manually sets the system date and time	GC	6-30
sntp-server daylight-saving	Sets the start and end dates for daylight savings time	GC	6-31
sntp-server timezone	Sets the time zone for the access point's internal clock	GC	6-32
show sntp	Shows current SNTP configuration settings	Exec	6-32
System Status	Displays system configuration and version information		
show system	Displays system information	Exec	6-33
show version	Displays version information for the system	Exec	6-34

country

This command configures the access point's country code, which identifies the country of operation and sets the authorized radio channels.

Syntax

country <*country_code*>

country_code - A two character code that identifies the country of operation. See the following table for a full list of codes.

Country	Code	Country	Code	Country	Code	Country	Code
Albania	AL	Dominican Republic	DO	Kuwait	KW	Qatar	QA
Algeria	DZ	Ecuador	EC	Latvia	LV	Romania	RO
Argentina	AR	Egypt	EG	Lebanon	LB	Russia	RU
Armenia	AM	Estonia	EE	Liechtenstein	LI	Saudi Arabia	SA
Australia	AU	Finland	FI	Lithuania	LT	Singapore	SG
Austria	AT	France	FR	Luxembourg	LU	Slovak Republic	SK
Azerbaijan	AZ	Georgia	GE	Macao	MO	Slovenia	SI
Bahrain	BH	Germany	DE	Macedonia	MK	South Africa	ZA
Belarus	BY	Greece	GR	Malaysia	MY	Spain	ES
Belgium	BE	Guatemala	GT	Mexico	MX	Sweden	SE
Belize	BZ	Hong Kong	HK	Monaco	MC	Switzerland	CH
Bolivia	BO	Hungary	HU	Morocco	MA	Syria	SY
Brazil	BR	Iceland	IS	North America	NA	Taiwan	TW
Brunei Darussalam	BN	India	IN	Netherlands	NL	Thailand	TH
Bulgaria	BG	Indonesia	ID	New Zealand	NZ	Turkey	TR

Country	Code	Country	Code	Country	Code	Country	Code
Canada	CA	Iran	IR	Norway	NO	Ukraine	UA
Chile	CL	Ireland	IE	Oman	OM	United Arab Emirates	AE
China	CN	Israel	IL	Pakistan	PK	United Kingdom	GB
Colombia	CO	Italy	IT	Panama	PA	United States	US
Costa Rica	CR	Japan	JP	Peru	PE	Uruguay	UY
Croatia	HR	Jordan	JO	Philippines	PH	Venezuela	VE
Cyprus	CY	Kazakhstan	KZ	Poland	PL	Vietnam	VN
Czech Republic	CZ	North Korea	KP	Portugal	PT		
Denmark	DK	Korea Republic	KR	Puerto Rico	PR		

Default Setting

US - for units sold in the United States
99 (no country set) - for units sold in other countries

Command Mode

Exec

Command Usage

- If you purchased an access point outside of the United States, the country code must be set before radio functions are enabled.
- The available Country Code settings can be displayed by using the **country?** command.

Example

```
SMC-AP#country ie
SMC-AP#
```

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

SMC Enterprise AP

Command Mode

Global Configuration

Example

```
SMC Enterprise AP(config)#prompt RD2
RD2(config)#
```

system name

This command specifies or modifies the system name for this device. Use the **no** form to restore the default system name.

Syntax

system name *name*
no system name

name - The name of this host. (Maximum length: 32 characters)

Default Setting

Enterprise AP

Command Mode

Global Configuration

Example

```
SMC-AP(config)#system name SMC-AP
SMC-AP(config)#
```

username

This command configures the user name for management access.

Syntax

username *name*

name - The name of the user.
(Length: 3-16 characters, case sensitive)

Default Setting

admin

Command Mode

Global Configuration

Example

```
SMC-AP(config)#username bob
SMC-AP(config)#
```

password

After initially logging onto the system, you should set the password. Remember to record it in a safe place. Use the **no** form to reset the default password.

Syntax

password *password*
no password

password - Password for management access. (Length: 3-16 characters, case sensitive)

Default Setting

smcadmin

Command Mode

Global Configuration

Example

```
SMC-AP(config)#password smc
SMC-AP(config)#
```

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1024-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
SMC-AP(config)#ip http port 1024
SMC-AP(config)#
```

Related Commands

ip http server (page 6-23)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
SMC-AP(config)#ip http server
SMC-AP(config)#
```

Related Commands

ip http port (page 6-22)

logging on

This command controls logging of error messages; i.e., sending debug or error messages to memory. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to memory. You can use the **logging level** command to control the type of error messages that are stored in memory.

Example

```
SMC-AP(config)#logging on
SMC-AP(config)#
```

logging host

This command specifies a syslog server host that will receive logging messages. Use the **no** form to remove syslog server host.

Syntax

logging host <*host_name* | *host_ip_address*>
no logging host

- *host_name* - The name of a syslog server. (Range: 1-20 characters)
- *host_ip_address* - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Example

```
SMC-AP(config)#logging host 10.1.0.3
SMC-AP(config)#
```

logging console

This command initiates logging of error messages to the console. Use the **no** form to disable logging to the console.

Syntax

logging console
no logging console

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
SMC-AP(config)#logging console
SMC-AP(config)#
```

logging level

This command sets the minimum severity level for event logging.

Syntax

logging level <**Alert** | **Critical** | **Error** | **Warning** | **Notice** | **Informational** | **Debug**>

Default Setting

Error

Command Mode

Global Configuration

Command Usage

Messages sent include the selected level down to Alert level.

Level Argument	Description
Alerts	Immediate action needed
Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
Error	Error conditions (e.g., invalid input, default used)
Warning	Warning conditions (e.g., return false, unexpected return)
Notice	Normal but significant condition, such as cold start
Informational	Informational messages only
Debug	Debugging messages

* There are only Critical, Notice, and Informational messages for the current firmware.

Example

```
SMC-AP(config)#logging level alert
SMC-AP(config)#
```

logging facility-type

This command sets the facility type for remote logging of syslog messages.

Syntax

logging facility-type <*type*>

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

16

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the access point. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
SMC-AP(config)#logging facility 19
SMC-AP(config)#
```

show logging

This command displays the logging configuration.

Syntax

show logging

Command Mode

Exec

Example

```
SMC-AP#show logging

Logging Information
==========================================
Syslog State                : Disabled
Logging Host State          : Enabled
Logging Console State       : Disabled
Server Domain name/IP       : none
Logging Level               : Error
Logging Facility Type       : 16
==========================================

SMC-AP#
```

sntp-server ip

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp-server ip <**1** | **2**> <*ip*>

- **1** - First time server.
- **2** - Second time server.
- *ip* - IP address of an time server (NTP or SNTP).

Default Setting

137.92.140.80
192.43.244.18

Command Mode

Global Configuration

Command Usage

When SNTP client mode is enabled using the **sntp-server enable** command, the **sntp-server ip** command specifies the time servers from which the access point polls for time updates. The access point will poll the time servers in the order specified until a response is received.

Example

```
SMC-AP(config)#sntp-server ip 10.1.0.19
SMC-AP#
```

Related Commands

sntp-server enable (page 6-29)
show sntp (page 6-32)

sntp-server enable

This command enables SNTP client requests for time synchronization with NTP or SNTP time servers specified by the **sntp-server ip** command. Use the **no** form to disable SNTP client requests.

Syntax

sntp-server enable
no sntp-server enable

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the access point only records the time starting from the factory default set at the last bootup (i.e., 00:14:00, January 1, 1970).

Example

```
SMC-AP(config)#sntp-server enable
SMC-AP(config)#
```

Related Commands

sntp-server ip (page 6-28)
show sntp (page 6-32)

sntp-server date-time

This command sets the system clock.

Default Setting

00:14:00, January 1, 1970

Command Mode

Global Configuration

Example

This example sets the system clock to 17:37 January 10, 2004.

```
SMC-AP#sntp-server date-time
Enter Year<1970-2100>: 2004
Enter Month<1-12>: 6
Enter Day<1-31>: 19
Enter Hour<0-23>: 17
Enter Min<0-59>: 37
SMC-AP#
```

Related Commands

sntp-server enable (page 6-29)

sntp-server daylight-saving

This command sets the start and end dates for daylight savings time. Use the **no** form to disable daylight savings time.

Syntax

sntp-server daylight-saving
no sntp-server daylight-saving

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The command sets the system clock back one hour during the specified period.

Example

This sets daylight savings time to be used from July 1st to September 1st.

```
SMC-AP(config)#sntp-server daylight-saving
Enter Daylight saving from which month<1-12>: 6
and which day<1-31>: 1
Enter Daylight saving end to which month<1-12>: 9
and which day<1-31>: 1
SMC-AP(config)#
```

sntp-server timezone

This command sets the time zone for the access point's internal clock.

Syntax

sntp-server timezone <*hours*>

hours - Number of hours before/after UTC.
(Range: -12 to +12 hours)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
SMC-AP(config)#sntp-server timezone +8
SMC-AP(config)#
```

show sntp

This command displays the current time and configuration settings for the SNTP client.

Command Mode

Exec

Example

```
SMC-AP#show sntp

SNTP Information
============================================================
Service State         : Enabled
SNTP (server 1) IP    : 137.92.140.80
SNTP (server 2) IP    : 192.43.244.18
Current Time          : 08 : 04, Jan 10th, 2004
Time Zone             : +8 (TAIPEI, BEIJING)
Daylight Saving       : Enabled, from Jun, 1st to Sep, 1st
============================================================

SMC-AP#
```

show system

This command displays basic system configuration settings.

Default Setting

None

Command Mode

Exec

Example

```
SMC-AP#show system
System Information
============================================================
Serial Number       : A341042933
System Up time      : 0 days, 1 hours, 8 minutes, 9 seconds
System Name         : SMC-AP
System Location     :
System Contact      : Contact
System Country Code : IE - IRELAND
MAC Address         : 00-04-E2-9C-74-8A
IP Address          : 192.168.2.2
Subnet Mask         : 255.255.255.0
Default Gateway     : 0.0.0.0
VLAN State          : DISABLED
IAPP State          : ENABLED
DHCP Client         : ENABLED
HTTP Server         : ENABLED
HTTP Server Port    : 80
Slot Status         : 802.11g only
Software Version    : v2.0.22
============================================================

SMC-AP#
```

show version

This command displays the software version for the system.

Default Setting

None

Command Mode

Exec

Example

```
SMC-AP#show version
Version v2.0.22
SMC-AP#
```

SNMP Commands

Controls access to this access point from management stations using the Simple Network Management Protocol (SNMP), as well as the hosts that will receive trap messages.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	6-35
snmp-server contact	Sets the system contact string	GC	6-36
snmp-server enable server	Enables SNMP service and traps	GC	6-37
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	6-38
snmp-server location	Sets the system location string	GC	6-39
show snmp	Displays the status of SNMP communications	Exec	6-40

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 23 characters, case sensitive)

- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

If you enter a community string without the **ro** or **rw** option, the default is read only.

Example

```
SMC-AP(config)#snmp-server community alpha rw
SMC-AP(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact. (Maximum length: 255 characters)

Default Setting

Contact

Command Mode

Global Configuration

Example

```
SMC-AP(config)#snmp-server contact Paul
SMC-AP(config)#
```

Related Commands

snmp-server location (page 6-39)

snmp-server enable server

This command enables SNMP management access and also enables this device to send SNMP traps (i.e., notifications). Use the **no** form to disable SNMP service and trap messages.

Syntax

snmp-server enable server
no snmp-server enable server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- This command enables both authentication failure notifications and link-up-down notifications.
- The **snmp-server host** command specifies the host device that will receive SNMP notifications.

Example

```
SMC-AP(config)#snmp-server enable server
SMC-AP(config)#
```

Related Commands

snmp-server host (page 6-38)

snmp-server host

This command specifies the recipient of an SNMP notification. Use the **no** form to remove the specified host.

Syntax

snmp-server host <*host_ip_address* | *host_name*> <*community-string*>
no snmp-server host

- *host_ip_address* - IP of the host (the targeted recipient).
- *host_name* - Name of the host. (Range: 1-20 characters)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 23 characters)

Default Setting

Host Address: None
Community String: public

Command Mode

Global Configuration

Command Usage

The **snmp-server host** command is used in conjunction with the **snmp-server enable server** command to enable SNMP notifications.

Example

```
SMC-AP(config)#snmp-server host 10.1.19.23 batman
SMC-AP(config)#
```

Related Commands

snmp-server enable server (page 6-37)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
SMC-AP(config)#snmp-server location WC-19
SMC-AP(config)#
```

Related Commands

snmp-server contact (page 6-36)

show snmp

This command displays the SNMP configuration settings.

Command Mode

Exec

Example

```
SMC-AP#show snmp

SNMP Information
=========================================
Service State  : Enable
Community (ro) : *****
Community (rw) : *****
Location       : WC-19
Contact        : Paul
Traps          : Enabled
Host Name/IP   : 10.1.19.23
Trap Community : *****
=========================================

SMC-AP#
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
bootfile	Specifies the file or image used to start up the system	GC	6-41
copy	Copies a code image or configuration between flash memory and a FTP/ TFTP server	Exec	6-42
delete	Deletes a file or code image	Exec	6-43
dir	Displays a list of files in flash memory	Exec	6-44

bootfile

This command specifies the image used to start up the system.

Syntax

bootfile <*filename*>

filename - Name of the image file.

Default Setting

None

Command Mode

Exec

Command Usage

- The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- If the file contains an error, it cannot be set as the default file.

Example

```
SMC-AP#bootfile smc-img.bin
SMC-AP#
```

copy

This command copies a boot file, code image, or configuration file between the access point's flash memory and a FTP/TFTP server. When you save the configuration settings to a file on a FTP/TFTP server, that file can later be downloaded to the access point to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax

copy <**ftp** | **tftp**> **file**
copy config <**ftp** | **tftp**>

- **ftp** - Keyword that allows you to copy to/from an FTP server.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **file** - Keyword that allows you to copy to/from a flash memory file.
- **config** - Keyword that allows you to upload the configuration file from flash memory.

Default Setting

None

Command Mode

Exec

Command Usage

- The system prompts for data required to complete the copy command.
- Only a configuration file can be uploaded to an FTP/TFTP server, but every type of file can be downloaded to the access point.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the FTP/TFTP

server is 255 characters or 32 characters for files on the access point. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the access point supports only two operation code files.
- The system configuration file must be named "syscfg" in all copy commands.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
SMC-AP#copy config tftp
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
SMC-AP#
```

The following example shows how to download a configuration file:

```
SMC-AP#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>:  [1]:2
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
SMC-AP#
```

delete

This command deletes a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Exec

Note: Beware of deleting application images from flash memory. At least one application image is required in order to boot the access point. If there are multiple image files in flash memory, and the one used to boot the access point is deleted, be sure you first use the **bootfile** command to update the application image file booted at startup before you reboot the access point.

Example

This example shows how to delete the test.cfg configuration file from flash memory.

```
SMC-AP#delete test.cfg
Are you sure you wish to delete this file? <y/n>:
SMC-AP#
```

Related Commands

bootfile (page 6-41)
dir (page 6-44)

dir

This command displays a list of files in flash memory.

Command Mode

Exec

Command Usage

File information is shown below:

Column Heading	Description
File Name	The name of the file.
Type	(2) Operation Code and (5) Configuration file
File Size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
SMC-AP#dir
File Name                       Type   File Size
--------------------------      ----  -----------
dflt-img.bin                      2     1044140
smc-img.bin                       2     1068532
syscfg                            5       16860
syscfg_bak                        5       16860

     1048576 byte(s) available

SMC-AP#
```

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access for RADIUS-aware devices to the network. An authentication server contains a database of credentials, such as users names and passwords, for each wireless client that requires access to the access point.

Command	Function	Mode	Page
radius-server address	Specifies the RADIUS server	GC	6-46
radius-server port	Sets the RADIUS server network port	GC	6-46
radius-server key	Sets the RADIUS encryption key	GC	6-47
radius-server retransmit	Sets the number of retries	GC	6-47
radius-server timeout	Sets the interval between sending authentication requests	GC	6-48
show radius	Shows the current RADIUS settings	Exec	6-49

radius-server address

This command specifies the primary and secondary RADIUS servers.

Syntax

radius-server address [**secondary**] <*host_ip_address* | *host_name*>

- **secondary** - Secondary server.
- *host_ip_address* - IP address of server.
- *host_name* - Host name of server. (Range: 1-20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
SMC-AP(config)#radius-server address 192.168.1.25
SMC-AP(config)#
```

radius-server port

This command sets the RADIUS server network port.

Syntax

radius-server [**secondary**] **port** <*port_number*>

- **secondary** - Secondary server.
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1024-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
SMC-AP(config)#radius-server port 1812
SMC-AP(config)#
```

radius-server key

This command sets the RADIUS encryption key.

Syntax

radius-server [**secondary**] **key** <*key_string*>

- **secondary** - Secondary server.
- *key_string* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

DEFAULT

Command Mode

Global Configuration

Example

```
SMC-AP(config)#radius-server key green
SMC-AP(config)#
```

radius-server retransmit

This command sets the number of retries.

Syntax

radius-server [**secondary**] **retransmit** *number_of_retries*

- **secondary** - Secondary server.
- *number_of_retries* - Number of times the access point will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

3

Command Mode

Global Configuration

Example

```
SMC-AP(config)#radius-server retransmit 5
SMC-AP(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server.

Syntax

radius-server [**secondary**] **timeout** *number_of_seconds*

- **secondary** - Secondary server.
- *number_of_seconds* - Number of seconds the access point waits for a reply before resending a request. (Range: 1-60)

Default Setting

5

Command Mode

Global Configuration

Example

```
SMC-AP(config)#radius-server timeout 10
SMC-AP(config)#
```

show radius

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Exec

Example

```
SMC-AP#show radius

Radius Server Information
========================================
IP               : 192.168.1.25
Port             : 1812
Key              : *****
Retransmit       : 5
Timeout          : 10
========================================

Radius Secondary Server Information
========================================
IP               : 0.0.0.0
Port             : 1812
Key              : *****
Retransmit       : 3
Timeout          : 5
========================================
SMC-AP#
```

802.1x Port Authentication

The access point supports IEEE 802.1x access control for wireless clients. This control feature prevents unauthorized access to the network by requiring a 802.1x client application to submit user credentials for authentication. Client authentication is then verified via by a RADIUS server using EAP (Extensible Authentication Protocol) before the access point grants client access to the network.

Command	Function	Mode	Page
802.1x	Configures 802.1x as disabled, supported, or required	GC	6-51
802.1x broadcast-key-refresh-rate	Sets the interval at which the primary broadcast keys are refreshed for stations using 802.1x dynamic keying	GC	6-52
802.1x session-key-refresh-rate	Sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying	GC	6-53
802.1x session-timeout	Sets the timeout after which a connected client must be re-authenticated	GC	6-54
address filter default	Sets filtering to allow or deny listed addresses	GC	6-54
address filter entry	Enters a MAC address in the filter table	GC	6-55
address filter delete	Removes a MAC address from the filter table	GC	6-56
mac-authentication server	Sets address filtering to be performed with local or remote options	GC	6-57

Command	Function	Mode	Page
mac-authentication session-timeout	Sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database	GC	6-58
show authentication	Shows all 802.1x authentication settings, as well as the address filter table	Exec	6-59

802.1x

This command configures 802.1x as optionally supported or as required for wireless clients. Use the **no** form to disable 802.1x support.

Syntax

802.1x <**supported** | **required**>
no 802.1x

- **supported** - Authenticates clients that initiate the 802.1x authentication process. Uses standard 802.11 authentication for all others.
- **required** - Requires 802.1x authentication for all clients.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- When 802.1x is disabled, the access point does not support 802.1x authentication for any station. After successful 802.11 association, each client is allowed to access the network.
- When 802.1x is supported, the access point supports 802.1x authentication only for clients initiating the 802.1x

authentication process (i.e., the access point does NOT initiate 802.1x authentication). For stations initiating 802.1x, only those stations successfully authenticated are allowed to access the network. For those stations not initiating 802.1x, access to the network is allowed after successful 802.11 association.

- When 802.1x is required, the access point enforces 802.1x authentication for all 802.11 associated stations. If 802.1x authentication is not initiated by the station, the access point will initiate authentication. Only those stations successfully authenticated with 802.1x are allowed to access the network.
- 802.1x does not apply to the 10/100Base-TX port.

Example

```
SMC-AP(config)#802.1x supported
SMC-AP(config)#
```

802.1x broadcast-key-refresh-rate

This command sets the interval at which the broadcast keys are refreshed for stations using 802.1x dynamic keying.

Syntax

802.1x broadcast-key-refresh-rate <*rate*>

rate - The interval at which the access point rotates broadcast keys. (Range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Global Configuration

Command Usage

- The access point uses EAPOL (Extensible Authentication Protocol Over LANs) packets to pass dynamic unicast session and broadcast keys to wireless clients. The 802.1x **broadcast-key-refresh-rate** command specifies the interval after which the broadcast keys are changed. The **802.1x session-key-refresh-rate** command specifies the interval after which unicast session keys are changed.
- Dynamic broadcast key rotation allows the access point to generate a random group key and periodically update all key-management capable wireless clients.

Example

```
SMC-AP(config)#802.1x broadcast-key-refresh-rate 5
SMC-AP(config)#
```

802.1x session-key-refresh-rate

This command sets the interval at which unicast session keys are refreshed for associated stations using dynamic keying.

Syntax

802.1x session-key-refresh-rate <*rate*>

rate - The interval at which the access point refreshes a session key. (Range: 0 - 1440 minutes)

Default Setting

0 (Disabled)

Command Mode

Global Configuration

Command Usage

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Example

```
SMC-AP(config)#802.1x session-key-refresh-rate 5
SMC-AP(config)#
```

802.1x session-timeout

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form to disable 802.1x re-authentication.

Syntax

802.1x session-timeout <*seconds*>
no 802.1x session-timeout

seconds - The number of seconds. (Range: 0-65535)

Default

0 (Disabled)

Command Mode

Global Configuration

Example

```
SMC-AP(config)#802.1x session-timeout 300
SMC-AP(config)#
```

address filter default

This command sets filtering to allow or deny listed MAC addresses.

Syntax

address filter default <**allowed** | **denied**>

- **allowed** - Only MAC addresses entered as “denied” in the address filtering table are denied.
- **denied** - Only MAC addresses entered as “allowed” in the address filtering table are allowed.

Default

allowed

Command Mode

Global Configuration

Example

```
SMC-AP(config)#address filter default denied
SMC-AP(config)#
```

Related Commands

address filter entry (page 6-55)
show authentication (page 6-59)

address filter entry

This command enters a MAC address in the filter table.

Syntax

address filter entry <*mac-address*> <**allowed** | **denied**>

- *mac-address* - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens; e.g., 00-90-D1-12-AB-89.)
- **allowed** - Entry is allowed access.
- **denied** - Entry is denied access.

Default

None

Command Mode

Global Configuration

Command Mode

- The access point supports up to 1024 MAC addresses.

- An entry in the address table may be allowed or denied access depending on the global setting configured for the **address entry default** command.

Example

```
SMC-AP(config)#address filter entry 00-70-50-cc-99-1a
 allowed
SMC-AP(config)#
```

Related Commands

address filter default (page 6-54)
show authentication (page 6-59)

address filter delete

This command deletes a MAC address from the filter table.

Syntax

address filter delete <*mac-address*>

mac-address - Physical address of client. (Enter six pairs of hexadecimal digits separated by hyphens.)

Default

None

Command Mode

Global Configuration

Example

```
SMC-AP(config)#address filter delete 00-70-50-cc-99-1b
SMC-AP(config)#
```

Related Commands

show authentication (page 6-59)

mac-authentication server

This command sets address filtering to be performed with local or remote options. Use the **no** form to disable MAC address authentication.

Syntax

mac-authentication server [**local** | **remote**]

- **local** - Authenticate the MAC address of wireless clients with the local authentication database during 802.11 association.
- **remote** - Authenticate the MAC address of wireless clients with the RADIUS server.

Default

local

Command Mode

Global Configuration

Example

```
SMC-AP(config)#mac-authentication server remote
SMC-AP(config)#
```

Related Commands

address filter entry (page 6-55)
radius-server address (page 6-46)
show authentication (page 6-59)

mac-authentication session-timeout

This command sets the interval at which associated clients will be re-authenticated with the RADIUS server authentication database. Use the **no** form to disable reauthentication.

Syntax

mac-authentication session-timeout <*seconds*>

seconds - Re-authentication interval. (Range: 0-65535)

Default

0 (disabled)

Command Mode

Global Configuration

Example

```
SMC-AP(config)#mac-authentication session-timeout 1
SMC-AP(config)#
```

show authentication

This command shows all 802.1x authentication settings, as well as the address filter table.

Command Mode

Exec

Example

```
SMC-AP#show authentication

Authentication Information
============================================================
MAC Authentication Server      : REMOTE
MAC Auth Session Timeout Value : 1 secs
802.1x                         : SUPPORTED
Broadcast Key Refresh Rate     : 5 min
Session Key Refresh Rate       : 5 min
802.1x Session Timeout Value   : 300 secs
Address Filtering              : DENIED

System Default : DENY addresses not found in filter table.
Filter Table

MAC Address             Status
-----------------       ----------
00-70-50-cc-99-1a       DENIED
00-70-50-cc-99-1b       ALLOWED
============================================================
SMC-AP(config)#
```

Filtering Commands

The commands described in this section are used to filter communications between wireless clients, control access to the management interface from wireless clients, and filter traffic using specific Ethernet protocol types.

Command	Function	Mode	Page
filter local-bridge	Disables communication between wireless clients	GC	6-60
filter ap-manage	Prevents wireless clients from accessing the management interface	GC	6-61
filter ethernet-type enable	Checks the Ethernet type for all incoming and outgoing Ethernet packets against the protocol filtering table	GC	6-62
filter ethernet-type protocol	Sets a filter for a specific Ethernet type	GC	6-63
show filter	Shows the filter configuration	Exec	6-64

filter local-bridge

This command disables communication between wireless clients. Use the **no** form to disable this filtering.

Syntax

filter local-bridge
no filter local-bridge

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command can disable wireless-to-wireless communications between clients via the access point. However, it does not affect communications between wireless clients and the wired network.

Example

```
SMC-AP(config)#filter local-bridge
SMC-AP(config)#
```

filter ap-manage

This command prevents wireless clients from accessing the management interface on the access point. Use the **no** form to disable this filtering.

Syntax

filter ap-manage
no filter ap-manage

Default

Disabled

Command Mode

Global Configuration

Example

```
SMC-AP(config)#filter ap-manage
SMC-AP(config)#
```

filter ethernet-type enable

This command checks the Ethernet type on all incoming and outgoing Ethernet packets against the protocol filtering table. Use the **no** form to disable this feature.

Syntax

filter ethernet-type enable
no filter ethernet-type enable

Default

Disabled

Command Mode

Global Configuration

Command Usage

This command is used in conjunction with the **filter ethernet-type protocol** command to determine which Ethernet protocol types are to be filtered.

Example

```
SMC-AP(config)#filter ethernet-type enable
SMC-AP(config)#
```

Related Commands

filter ethernet-type protocol (page 6-63)

filter ethernet-type protocol

This command sets a filter for a specific Ethernet type. Use the **no** form to disable filtering for a specific Ethernet type.

Syntax

filter ethernet-type protocol <*protocol*>
no filter ethernet-type protocol <*protocol*>

protocol - An Ethernet protocol type. (Options: ARP, RARP, Berkeley-Trailer-Negotiation, LAN-Test, X25-Level-3, Banyan, CDP, DEC XNS, DEC-MOP-Dump-Load, DEC-MOP, DEC-LAT, Ethertalk, Appletalk-ARP, Novell-IPX(old), Novell-IPX(new), EAPOL, Telxon-TXP, Aironet-DDP, Enet-Config-Test)

Default

None

Command Mode

Global Configuration

Command Usage

Use the **filter ethernet-type enable** command to enable filtering for Ethernet types specified in the filtering table, or the no **filter ethernet-type enable** command to disable all filtering based on the filtering table.

Example

```
SMC-AP(config)#filter ethernet-type protocol ARP
SMC-AP(config)#
```

Related Commands

filter ethernet-type enable (page 6-62)

show filters

This command shows the filter options and protocol entries in the filter table.

Command Mode

Exec

Example

```
SMC-AP#show filters

Protocol Filter Information
============================================================
Local Bridge          :ENABLED
AP Management         :ENABLED
Ethernet Type Filter :ENABLED

Enabled Protocol Filters
------------------------------------------------------------
Protocol: ARP                                ISO: 0x0806
============================================================
SMC-AP#
```

Interface Commands

The commands described in this section configure connection parameters for the Ethernet port and wireless interface.

Command	Function	Mode	Page
General Interface			
interface	Enters specified interface configuration mode	GC	6-68
Ethernet Interface			
dns primary-server	Specifies the primary name server	IC-E	6-68
dns secondary-server	Specifies the secondary name server	IC-E	6-68
ip address	Sets the IP address for the Ethernet interface	IC-E	6-69
ip dhcp	Submits a DHCP request for an IP address	IC-E	6-71
shutdown	Disables the Ethernet interface	IC-E	6-72
show interface ethernet	Shows the status for the Ethernet interface	Exec	6-72
Wireless Interface			
radio-mode	Sets the radio working mode	IC-W	6-73
select-antenna-mode	Selects built-in antennas or optional high-gain antenna	IC-W	6-74
description	Adds a description to the wireless interface	IC-W	6-73
ssid-broadcast	Opens access to clients without a pre-configured SSID	IC-W	6-75

Command	Function	Mode	Page
speed	Configures the maximum data rate at which a station can connect to the access point	IC-W	6-76
channel	Configures the radio channel	IC-W	6-77
ssid	Configures the service set identifier	IC-W	6-78
beacon-interval	Configures the rate at which beacon signals are transmitted from the access point	IC-W	6-78
dtim-period	Configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions	IC-W	6-79
fragmentation-length	Configures the minimum packet size that can be fragmented	IC-W	6-80
rts-threshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications	IC-W	6-81
authentication	Defines the 802.11 authentication type allowed by the access point	IC-W	6-82
encryption	Defines whether or not WEP encryption is used to provide privacy for wireless communications	IC-W	6-83
key	Sets the keys used for WEP encryption	IC-W	6-84

Command	Function	Mode	Page
transmit-key	Sets the index of the key to be used for encrypting data frames sent between the access point and wireless clients	IC-W	6-85
transmit-power	Adjusts the power of the radio signals transmitted from the access point	IC-W	6-86
max-association	Configures the maximum number of clients that can be associated with the access point at the same time	IC-W	6-87
multicast-cipher	Defines the cipher algorithm used for multicasting	IC-W	6-88
wpa-clients	Defines whether WPA is required or optionally supported for client stations	IC-W	6-89
wpa-mode	Specifies dynamic keys or a pre-shared key	IC-W	6-91
wpa-preshared-key	Defines a WPA preshared-key value	IC-W	6-92
wpa-psk-type	Defines the type of the preshared-key	IC-W	6-93
shutdown	Disables the wireless interface	IC-W	6-94
show interface wireless	Shows the status for the wireless interface	Exec	6-95
show station	Shows the wireless clients associated with the access point	Exec	6-96

interface

This command configures an interface type and enters interface configuration mode.

Syntax

interface <**ethernet** | **wireless** <**g**>>

- **ethernet** - Interface for wired network.
- **wireless** - Interface for wireless clients.
  - **g** - 802.11g radio interface.

Default Setting

None

Command Mode

Global Configuration

Example

To specify the 10/100Base-TX network interface, enter the following command:

```
SMC-AP(config)#interface ethernet
SMC-AP(if-ethernet)#
```

dns server

This command specifies the address for the primary or secondary domain name server to be used for name-to-address resolution.

Syntax

dns primary-server <*server-address*>
dns secondary-server <*server-address*>

- **primary-server** - Primary server used for name resolution.
- **secondary-server** - Secondary server used for name resolution.
- *server-address* - IP address of domain-name server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The primary and secondary name servers are queried in sequence.

Example

This example specifies two domain-name servers.

```
SMC-AP(if-ethernet)#dns primary-server 192.168.1.55
SMC-AP(if-ethernet)#dns secondary-server 10.1.0.55
SMC-AP(if-ethernet)#
```

Related Commands

show interface ethernet (page 6-72)

ip address

This command sets the IP address for the (10/100Base-TX) Ethernet interface. Use the **no** form to restore the default IP address.

Syntax

ip address <*ip-address*> <*netmask*> <*gateway*>
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- *gateway* - IP address of the default gateway

Default Setting

IP address: 192.168.2.2
Netmask: 255.255.255.0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- DHCP is enabled by default. To manually configure a new IP address, you must first disable the DHCP client with the **no ip dhcp** command.
- You must assign an IP address to this device to gain management access over the network or to connect the access point to existing IP subnets. You can manually configure a specific IP address using this command, or direct the device to obtain an address from a DHCP server using the **ip dhcp** command. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

Example

```
SMC-AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
SMC-AP(if-ethernet)#ip address 192.168.2.2 255.255.255.0
 192.168.1.253
SMC-AP(if-ethernet)#
```

Related Commands

ip dhcp (page 6-71)

ip dhcp

This command sets the IP address for the currently selected ethernet interface. Use the **no** form to restore the default IP address.

Syntax

ip dhcp
no ip dhcp

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the access point to existing IP subnets. You can manually configure a specific IP address using the **ip address** command, or direct the device to obtain an address from a DHCP server using this command.
- When you use this command, the access point will begin broadcasting DHCP client requests. The current IP address (i.e., default or manually configured address) will continue to be effective until a DHCP reply is received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (DHCP values can include the IP address, subnet mask, and default gateway.)

Example

```
SMC-AP(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
SMC-AP(if-ethernet)#ip dhcp
SMC-AP(if-ethernet)#
```

Related Commands

ip address (page 6-69)

shutdown

This command disables the Ethernet interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command allows you to disable the Ethernet port due to abnormal behavior (e.g., excessive collisions), and reenable it after the problem has been resolved. You may also want to disable the Ethernet port for security reasons.

Example

The following example disables the Ethernet port.

```
SMC-AP(if-ethernet)#shutdown
SMC-AP(if-ethernet)#
```

show interface ethernet

This command displays the status for the Ethernet interface.

Syntax

show interface [**ethernet**]

Default Setting

Ethernet interface

Command Mode

Exec

Example

```
SMC-AP#show interface ethernet
Ethernet Interface Information
=======================================
IP Address          : 192.168.2.2
Subnet Mask         : 255.255.255.0
Default Gateway     : 0.0.0.0
Primary DNS         : 192.168.1.55
Secondary DNS       : 10.1.0.55
Admin status        : Up
Operational status  : Up
=======================================
SMC-AP#
```

radio-mode

This command sets the working mode for the wireless interface.

Syntax

radio-mode <**b** | **g** | **b+g**>

- b - b-only mode: Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
- g - g-only mode: Only 802.11g clients can communicate with the access point.
- b+g - b & g mixed mode: Both 802.11b and 802.11g clients can communicate with the access point.

Default Setting

b & g mixed mode

Command Mode

Interface Configuration (Wireless g)

Example

```
SMC-AP(config)#interface wireless g
SMC-AP(if-wireless g)#radio-mode g
SMC-AP(if-wireless g)#
```

select-antenna-mode

This command selects the built-in antennas or an optional high-gain antenna attached to the socket on the right antenna.

Syntax

select-antenna-mode <**diversity** | **right antenna**>

- **diversity** - Selects the built-in antennas. The transmitted signal is sent out both antennas, and the antenna with the best incoming signal is used for reception.
- **right antenna** - The right antenna is used both for transmission and reception. Use this setting when an optional high-gain antenna is attached to the access point.

Default Setting

diversity

Command Mode

Interface Configuration (Wireless g)

Example

```
SMC-AP(config)#interface wireless g
SMC-AP(if-wireless g)#select-antenna-mode right
SMC-AP(if-wireless g)#
```

description

This command adds a description to a the wireless interface. Use the **no** form to remove the description.

Syntax

description <*string*>
no description

string - Comment or a description for this interface. (Range: 1-80 characters)

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Example

```
SMC-AP(config)#interface wireless g
SMC-AP(if-wireless g)#description RD-AP#3
SMC-AP(if-wireless g)#
```

ssid-broadcast

This command opens access to clients without a pre-configured SSID. Use the **no** form to disable this feature.

Syntax

ssid-broadcast
no ssid-broadcast

Default Setting

Enabled

Command Mode

Interface Configuration (Wireless)

Command Usage

When SSID broadcast is disabled, the access point will not include its SSID in beacon messages. Nor will it respond to probe requests from clients that do not include a fixed SSID.

Example

```
SMC-AP(if-wireless g)#no ssid-broadcast
SMC-AP(if-wireless g)#
```

speed

This command configures the maximum data rate at which a station can connect to the access point.

Syntax

speed <*speed*>

speed - Maximum access speed allowed for wireless clients. (Options: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps)

Default Setting

54 Mbps

Command Mode

Interface Configuration (Wireless)

Command Usage

The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. Please refer to the table for maximum distances on page A-4.

Example

```
SMC-AP(if-wireless g)#speed 6
SMC-AP(if-wireless g)#
```

channel

This command configures the radio channel through which the access point communicates with wireless clients.

Syntax

channel <*channel* | **auto**>

- *channel* - Manually sets the radio channel used for communications with wireless clients. (Range: 802.11g - 1 to 11 for US & Canada, 10 to 13 for France, 1 to 13 for rest of Europe, 1 to 14 for Japan)
- **auto** - Automatically selects an unoccupied channel (if available). Otherwise, the lowest channel is selected.

Default Setting

Automatic channel selection

Command Mode

Interface Configuration (Wireless)

Command Usage

- The available channel settings are limited by local regulations, which determine the number of channels that are available.
- When multiple access points are deployed in the same area, be sure to choose a channel separated by at least five channels for 802.11g to avoid having the channels interfere with each other. You can deploy up to three access points in the same area for 802.11g (e.g., channels 1, 6, 11).
- For most wireless adapters, the channel for wireless clients is automatically set to the same as that used by the access point to which it is linked.

Example

```
SMC-AP(if-wireless g)#channel 1
SMC-AP(if-wireless g)#
```

ssid

This command configures the service set identifier (SSID).

Syntax

ssid *string*

string - The name of a basic service set supported by the access point. (Range: 1 - 32 characters)

Default Setting

smc

Command Mode

Interface Configuration (Wireless)

Command Usage

Clients that want to connect to the wireless network via an access point must set their SSIDs to the same as that of the access point.

Example

```
SMC-AP(if-wireless g)#ssid RD-AP#3
SMC-AP(if-wireless g)#
```

beacon-interval

This command configures the rate at which beacon signals are transmitted from the access point.

Syntax

beacon-interval <*interval*>

interval - The rate for transmitting beacon signals. (Range: 20-1000 milliseconds)

Default Setting

100

Command Mode

Interface Configuration (Wireless)

Command Usage

The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information.

Example

```
SMC-AP(if-wireless g)#beacon-interval 150
SMC-AP(if-wireless g)#
```

dtim-period

This command configures the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

Syntax

dtim-period <*interval*>

interval - Interval between the beacon frames that transmit broadcast or multicast traffic. (Range: 1-255 beacon frames)

Default Setting

2

Command Mode

Interface Configuration (Wireless)

Command Usage

- The Delivery Traffic Indication Map (DTIM) packet interval value indicates how often the MAC layer forwards broadcast/multicast traffic. This parameter is necessary to wake up stations that are using Power Save mode.
- The DTIM is the interval between two synchronous frames with broadcast/multicast information. The default value of 2

indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.

- Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames.

Example

```
SMC-AP(if-wireless g)#dtim-period 100
SMC-AP(if-wireless g)#
```

fragmentation-length

This command configures the minimum packet size that can be fragmented when passing through the access point.

Syntax

fragmentation-length <*length*>

length - Minimum packet size for which fragmentation is allowed. (Range: 256-2346 bytes)

Default Setting

2346

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the packet size is smaller than the preset Fragment size, the packet will not be segmented.
- Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or

collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames.

Example

```
SMC-AP(if-wireless g)#fragmentation-length 512
SMC-AP(if-wireless g)#
```

rts-threshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving station prior to the sending station starting communications.

Syntax

rts-threshold <*threshold*>

threshold - Threshold packet size for which to send an RTS. (Range: 0-2347 bytes)

Default Setting

2347

Command Mode

Interface Configuration (Wireless)

Command Usage

- If the threshold is set to 0, the access point never sends RTS signals. If set to 2347, the access point always sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.
- The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an

RTS frame, the station sends a CTS frame to notify the sending station that it can start sending data.

- Access points contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node” problem.

Example

```
SMC-AP(if-wireless g)#rts-threshold 256
SMC-AP(if-wireless g)#
```

authentication

This command defines the 802.11 authentication type allowed by the access point.

Syntax

authentication <**open** | **shared**>

- **open** - Accepts the client without verifying its identity using a shared key.
- **shared** - Authentication is based on a shared key that has been distributed to all stations.

Default Setting

open

Command Mode

Interface Configuration (Wireless)

Command Usage

- Shared key authentication can only be used when WEP is enabled with the **encryption** command, and at least one static WEP key has been defined with the **key** command.
- When using WPA or 802.1x for authentication and dynamic keying, the access point must be set to **open**.

Example

```
SMC-AP(if-wireless g)#authentication shared
SMC-AP(if-wireless g)#
```

Related Commands

encryption (page 6-83)
key (page 6-84)

encryption

This command defines whether or not WEP encryption is used to provide privacy for wireless communications. Use the **no** form to disable encryption.

Syntax

encryption <*key-length*>
no encryption

key-length - Size of encryption key. (Options: 64, 128, or 152 bits)

Default Setting

disabled

Command Mode

Interface Configuration (Wireless)

Command Usage

- Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. For more secure data transmissions, enable WEP with this command, and set at least one static WEP key with the **key** command.
- The WEP settings must be the same on each client in your wireless network.
- The encryption length specified in the **encryption** command and the **key** command must match.

- Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Example

```
SMC-AP(if-wireless g)#encryption 128
SMC-AP(if-wireless g)#
```

Related Commands

key (page 6-84)

key

This command sets the keys used for WEP encryption. Use the **no** form to delete a configured key.

Syntax

key <*index*> <*size*> <*type*> <*value*>
no key *index*

- *index* - Key index. (Range: 1-4)
- *size* - Key size. (Options: 64, 128, or 152 bits)
- *type* - Input format. (Options: ASCII, HEX)
- *value* - The key string. For ASCII input, use 5/13 alphanumeric characters for 64/128 bit strings. For HEX input, use 10/26 hexadecimal digits for 64/128 bit strings.

Default Setting

None

Command Mode

Interface Configuration (Wireless)

Command Usage

- To enable Wired Equivalent Privacy (WEP), use the **authentication** command to select the “shared key” authentication type, use the **encryption** command to

specify the key length, and use the **key** command to configure at least one key.

- If WEP is enabled, all wireless clients must be configured with the same shared keys to communicate with the access point.
- The encryption length specified in the **encryption** command and the **key** command must match.
- The encryption index, length and type configured in the access point must match those configured in the clients.

Example

```
SMC-AP(if-wireless g)#key 1 128 hex 1234512345529
SMC-AP(if-wireless g)#key 2 128 ascii asdeipadjsipd
SMC-AP(if-wireless g)#key 3 128 hex 1234512345123
SMC-AP(if-wireless g)#
```

Related Commands

authentication (page 6-82)
encryption (page 6-83)

transmit-key

This command sets the index of the key to be used for encrypting data frames broadcast or multicast from the access point to wireless clients.

Syntax

transmit-key <*index*>

index - Key index. (Range: 1-4)

Default Setting

1

Command Mode

Interface Configuration (Wireless)

Command Usage

- If you use WEP key encryption, the access point uses the transmit key to encrypt multicast and broadcast data signals that it sends to client devices. Other keys can be used for decryption of data from clients.
- When using IEEE 802.1x, the access point uses a dynamic WEP key to encrypt unicast and broadcast messages to 802.1x-enabled clients. However, because the access point sends the WEP keys during the 802.1x authentication process, these keys do not have to appear in the client's WEP key list.

Example

```
SMC-AP(if-wireless g)#transmit-key 2
SMC-AP(if-wireless g)#
```

transmit-power

This command adjusts the power of the radio signals transmitted from the access point.

Syntax

transmit-power <*signal-strength*>

signal-strength - Signal strength transmitted from the access point. (Options: full, half, quarter, eighth, min)

Default Setting

full

Command Mode

Interface Configuration (Wireless)

Command Usage

- The "min" keyword indicates minimum power.
- The longer the transmission distance, the higher the transmission power required. But to support the maximum

number of users in an area, you must keep the power as low as possible. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high strength signals do not interfere with the operation of other radio devices in your area.

Example

```
SMC-AP(if-wireless g)#transmit-power half
SMC-AP(if-wireless g)#
```

max-association

This command configures the maximum number of clients that can be associated with the access point at the same time.

Syntax

max-association <*count*>

count - Maximum number of associated stations. (Range: 0-64)

Default Setting

64

Command Mode

Interface Configuration (Wireless)

Example

```
SMC-AP(if-wireless g)#max-association 32
SMC-AP(if-wireless g)#
```

multicast-cipher

This command defines the cipher algorithm used for broadcasting and multicasting when using Wi-Fi Protected Access (WPA) security.

Syntax

multicast-cipher <**AES** | **TKIP** | **WEP**>

- **AES** - Advanced Encryption Standard
- **TKIP** - Temporal Key Integrity Protocol
- **WEP** - Wired Equivalent Privacy

Default Setting

WEP

Command Mode

Interface Configuration (Wireless)

Command Usage

- WPA enables the access point to support different unicast encryption keys for each client. However, the global encryption key for multicast and broadcast traffic must be the same for all clients. This command sets the encryption type that is supported by all clients.
- If any clients supported by the access point are not WPA enabled, the multicast-cipher algorithm must be set to WEP.
- WEP is the first generation security protocol used to encrypt data crossing the wireless medium using a fairly short key. Communicating devices must use the same WEP key to encrypt and decrypt radio signals. WEP has many security flaws, and is not recommended for transmitting highly sensitive data.
- TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.

- TKIP defends against attacks on WEP in which the unencrypted initialization vector in encrypted packets is used to calculate the WEP key. TKIP changes the encryption key on each packet, and rotates not just the unicast keys, but the broadcast keys as well. TKIP is a replacement for WEP that removes the predictability that intruders relied on to determine the WEP key.
- AES has been designated by the National Institute of Standards and Technology as the successor to the Data Encryption Standard (DES) encryption algorithm, and will be used by the U.S. government for encrypting all sensitive, nonclassified information. Because of its strength, and resistance to attack, AES is also being incorporated as part of the 802.11 standard.

Example

```
SMC-AP(if-wireless g)#multicast-cipher TKIP
SMC-AP(if-wireless g)#
```

wpa-clients

This command defines whether Wi-Fi Protected Access (WPA) is required or optionally supported for client stations.

Syntax

wpa-clients <**required** | **supported**>

- **required** - Supports only clients using WPA.
- **supported** - Support clients with or without WPA.

Default Setting

Supported

Command Mode

Interface Configuration (Wireless)

Command Usage

Wi-Fi Protected Access (WPA) provides improved data encryption, which was weak in WEP, and user authentication, which was largely missing in WEP. WPA uses the following security mechanisms.

Enhanced Data Encryption through TKIP

WPA uses Temporal Key Integrity Protocol (TKIP). TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.

Enterprise-level User Authentication via 802.1x and EAP

To strengthen user authentication, WPA uses 802.1x and the Extensible Authentication Protocol (EAP). Used together, these protocols provide strong user authentication via a central RADIUS authentication server that authenticates each user on the network before they join it. WPA also employs “mutual authentication” to prevent a wireless client from accidentally joining a rogue network.

Example

```
SMC-AP(if-wireless g)#wpa-client required
SMC-AP(if-wireless g)#
```

Related Commands

wpa-mode (page 6-91)

wpa-mode

This command specifies whether Wi-Fi Protected Access (WPA) is to use 802.1x dynamic keys or a pre-shared key.

Syntax

wpa-mode <**dynamic** | **pre-shared-key**>

- **dynamic** - WPA with 802.1x dynamic keys.
- **pre-shared-key** - WPA with a pre-shared key.

Default Setting

dynamic

Command Mode

Interface Configuration (Wireless)

Command Usage

- When the WPA mode is set to “dynamic,” clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA-enabled or support 802.1x client software. A RADIUS server must also be configured and be available in the wired network.
- In the dynamic mode, keys are generated for each wireless client associating with the access point. These keys are regenerated periodically, and also each time the wireless client is re-authenticated.
- When the WPA mode is set to “pre-shared-key,” the key must first be generated and distributed to all wireless clients before they can successfully associate with the access point.

Example

```
SMC-AP(if-wireless g)#wpa-mode pre-shared-key
SMC-AP(if-wireless g)#
```

Related Commands

wpa-clients (page 6-89)
wpa-preshared-key (page 6-92)

wpa-preshared-key

This command defines a Wi-Fi Protected Access (WPA) preshared-key.

Syntax

wpa-preshared-key <*type*> <*value*>

- *type* - Input format. (Options: ASCII, HEX)
- *value* - The key string. For ASCII input, use 5/13 alphanumeric characters for 64/128 bit strings. For HEX input, use 10/26 hexadecimal digits for 64/128 bit strings.

Command Mode

Interface Configuration (Wireless)

Command Usage

- To support Wi-Fi Protected Access (WPA) for client authentication, use the **wpa-clients** command to specify the authentication type, use the **wpa-mode** command to specify pre-shared-key mode, and use this command to configure one static key.
- If WPA is used with pre-shared-key mode, all wireless clients must be configured with the same pre-shared key to communicate with the access point.

Example

```
SMC-AP(if-wireless g)#wpa-preshared-key ASCII agoodsecret
SMC-AP(if-wireless g)#
```

Related Commands

wpa-clients (page 6-89)
wpa-mode (page 6-91)

wpa-psk-type

This command defines the Wi-Fi Protected Access (WPA) preshared-key type.

Syntax

wpa-psk-type <*type*>

type - Input format. (Options: Alphanumeric, HEX)

Default Setting

HEX

Command Mode

Interface Configuration (Wireless)

Example

```
SMC-AP(if-wireless g)#wpa-preshared-key ASCII agoodsecret
SMC-AP(if-wireless g)#
```

Related Commands

wpa-preshared-key (page 6-92)

shutdown

This command disables the wireless interface. Use the **no** form to restart the interface.

Syntax

shutdown
no shutdown

Default Setting

Interface enabled

Command Mode

Interface Configuration (Wireless)

Example

```
SMC-AP(if-wireless g)#shutdown
SMC-AP(if-wireless g)#
```

show interface wireless

This command displays the status for the wireless interface.

Syntax

show interface wireless <g>

- **g** - 802.11g radio interface.

Command Mode

Exec

Example

```
SMC-AP#show interface wireless g

Wireless Interface Information
============================================================
---------------Identification--------------------------
Description                : Enterprise 802.11g Access Point
SSID                       : SMC-AP
Channel                    : 0 (AUTO)
Status                     : Disable
----------------802.11 Parameters-----------------------
Transmit Power             : HALF (10 dBm)
Max Station Data Rate      : 54Mbps
Fragmentation Threshold    : 2346 bytes
RTS Threshold              : 2347 bytes
Beacon Interval            : 100 TUs
DTIM Interval              : 2 beacons
Maximum Association        : 32 stations
----------------Security---------------------------------
SSID Broadcast             : DISABLED
Multicast cipher           : TKIP
Unicast cipher             : WEP
WPA clients                : SUPPORTED
Encryption                 : DISABLED
Default Transmit Key       : 1
Static Keys :
   Key 2: EMPTY    Key 3: EMPTY    Key 4: EMPTY
Authentication Type        : OPEN
============================================================
SMC-AP#
```

show station

This command shows the wireless clients associated with the access point.

Command Mode

Exec

Example

```
SMC-AP#show station
802.11g Station Table
Station Address   : 00-04-E2-41-C2-9D
        Authenticated        : TRUE
        Associated           : TRUE
        Forwarding Allowed   : TRUE
SMC-AP#
```

IAPP Commands

The command described in this section enables the protocol signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points. In other words, the 802.11f protocol can ensure successful roaming between access points in a multi-vendor environment.

iapp

This command enables the protocol signaling required to hand over wireless clients roaming between different 802.11f-compliant access points. Use the **no** form to disable 802.11f signaling.

Syntax

iapp
no iapp

Default

Enabled

Command Mode

Global Configuration

Command Usage

The current 802.11 standard does not specify the signaling required between access points in order to support clients roaming from one access point to another. In particular, this can create a problem for clients roaming between access points from different vendors. This command is used to enable or disable 802.11f handover signaling between different access points, especially in a multi-vendor environment.

Example

```
SMC-AP(config)#iapp
SMC-AP(config)#
```

VLAN Commands

The access point can enable the support of VLAN-tagged traffic passing between wireless clients and the wired network. Up to 16 VLAN IDs can be mapped to specific wireless clients, allowing users to remain within the same VLAN as they move around a campus site.

When VLAN is enabled on the access point, a VLAN ID (a number between 1 and 4095) can be assigned to each client after successful authentication using IEEE 802.1x and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the access point assigns the user to its own configured native VLAN ID.

Note: When VLANs are enabled, the access point's Ethernet port drops all received traffic that does not include a VLAN tag. To maintain network connectivity to the access point and wireless clients, be sure that the access point is connected to a device port that supports IEEE 802.1Q VLAN tags.

The VLAN commands supported by the access point are listed below.

Command	Function	Mode	Page
vlan	Enables a single VLAN for all traffic	GC	6-99
native-vlanid	Configures the native VLAN for the access point	GC	6-100

vlan

This command enables VLANs for all traffic. Use the **no** form to disable VLANs.

Syntax

vlan enable
no vlan

Default

Disabled

Command Mode

Global Configuration

Command Description

- When VLANs are enabled, the access point tags frames received from wireless clients with the VLAN ID configured for each client on the RADIUS server. If the VLAN ID has not been configured for a client on the RADIUS server, then the frames are tagged with the access point's native VLAN ID.
- Traffic entering the Ethernet port must be tagged with a VLAN ID that matches the access point's native VLAN ID, or with a VLAN tag that matches one of the wireless clients currently associated with the access point.

Example

```
SMC-AP(config)#vlan enable
Reboot system now? <y/n>: y
```

Related Commands

native-vlanid (page 6-100)

native-vlanid

This command configures the native VLAN ID for the access point.

Syntax

native-vlanid <*vlan-id*>

vlan-id - Native VLAN ID. (Range: 1-16)

Default Setting

1

Command Mode

Global Configuration

Command Usage

When VLANs are enabled on the access point, a VLAN ID (a number between 1 and 4095) can be assigned to each client after successful authentication using IEEE 802.1x and a central RADIUS server. If a wireless client does not have a VLAN ID configured on the RADIUS server, the access point assigns the user to its own configured native VLAN ID (a number between 1 and 16).

Example

```
SMC-AP(config)#native-vlanid 3
SMC-AP(config)#
```

Related Commands

vlan (page 6-99)

Appendix A Troubleshooting

Check the following items before you contact local Technical Support.

1. If wireless clients cannot access the network, check the following:
   - Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
   - If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
   - If authentication is being performed through a RADIUS server, ensure that the clients are properly configured on the RADIUS server.
   - If authentication is being performed through IEEE 802.1x, be sure the wireless users have installed and properly configured 802.1x client software.
   - If MAC address filtering is enabled, be sure the client's address is included in the local filtering database or on the RADIUS server database.
   - If the wireless clients are roaming between access points, make sure that all the access points and wireless devices in the Extended Service Set (ESS) are configured to the same SSID, and authentication method.

2. If the access point cannot be configured using the Telnet, a web browser, or SNMP software:
   - Be sure to have configured the access point with a valid IP address, subnet mask and default gateway.
   - If VLANs are enabled on the access point, the management station should be configured to send tagged frames with a VLAN ID that matches the access point's native VLAN (default VLAN 1, page 5-20). However, to manage the access point from a wireless client, the AP Management Filter should be disabled (page 5-20).
   - Check that you have a valid network connection to the access point and that the Ethernet port or the wireless interface that you are using has not been disabled.
   - If you are connecting to the access point through the wired Ethernet interface, check the network cabling between the management station and the access point. If you are connecting to access point from a wireless client, ensure that you have a valid connection to the access point.
   - If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (i.e, four sessions). Try connecting again at a later time.
3. If you cannot access the on-board configuration program via a serial port connection:
   - Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.
   - Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.

4. If you forgot or lost the password:
   - Set the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name “admin” with the password “smcadmin” to access the management interface.
5. If all other recovery measure fail, and the access point is still not functioning properly, take any of these steps:
   - Reset the access point’s hardware using the console interface, web interface, or through a power reset.
   - Reset the access point to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name “admin” with the password “smcadmin” to access the management interface.

Maximum Distance Table

Important Notice

Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those posted below.

802.11b Wireless Distance Table				
	Speed and Distance Ranges			
Environment	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Outdoors[1]	300 m 984 ft	465 m 1525 ft	500 m 1639 ft	515 m 1689 ft
Indoors[2]	60 m 197 ft	70 m 230 ft	83 m 272 ft	85 m 279 ft

802.11g Wireless Distance Table												
	Speed and Distance Ranges											
Environment	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	11 Mbps	9 Mbps	6 Mbps	5 Mbps	2 Mbps	1 Mbps
Outdoors[1]	82 m 269 ft	100 m 328 ft	300 m 984 ft	330 m 1082 ft	350 m 1148 ft	450 m 1475 ft	470 m 1541 ft	485 m 1590 ft	495 m 1623 ft	510 m 1672 ft	520 m 1705 ft	525 m 1722 ft
Indoors[2]	20 m 66 ft	25 m 82 ft	35 m 115 ft	43 m 141 ft	50 m 164 ft	57 m 187 ft	66 m 216 ft	71 m 233 ft	80 m 262 ft	85 m 279 ft	90 m 295 ft	93 m 305 ft

Notes:
1. Outdoor Environment: A line-of-sight environment with no interference or obstruction between the access point and clients.
2. Indoor Environment: A typical office or home environment with floor to ceiling obstructions between the access point and clients.

Appendix B
Cables and Pinouts

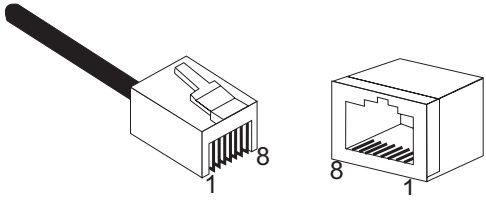
Twisted-Pair Cable Assignments

Caution: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (See “Straight-Through Wiring” on page B-3 and “Crossover Wiring” on page B-3 for an explanation.)

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 port on the access point is wired with MDI pinouts. This means that you must use crossover cables for connections to PCs or servers, and straight-through cable for connections to switches or hubs. However, when connecting to devices that support automatic MDI/MDI-X pinout configuration, you can use either straight-through or crossover cable.

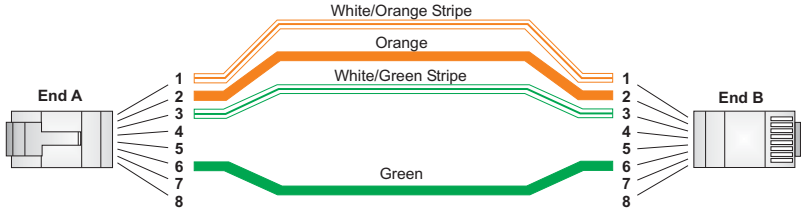
10/100BASE-TX MDI and MDI-X Port Pinouts		
Pin	**MDI-X Signal Name**	**MDI Signal Name**
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)
4,5,7,8	Not used	Not used

Note: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use “straight-through” cable for network connections to hubs or switches that only have MDI-X ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either “straight-through” or “crossover” cable.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Straight-through Cable



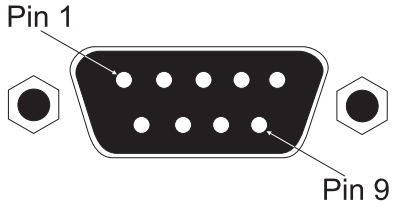
Crossover Wiring

Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use “crossover” cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either “straight-through” or “crossover” cable.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Crossover Cable

Console Port Pin Assignments

The DB-9 DCE serial port on the front panel of the SMC2552W-G is used to connect to the access point for out-of-band console configuration. The command-line configuration program can be accessed from a terminal, or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



Wiring Map for Serial Cable

Signal (serial port)	Pin	Signal (management console port)
Unused	1	Unused
TXD (transmit data)	2	RXD (receive data)
RXD (receive data)	3	TXD (transmit data)
Unused	4	Unused
GND (ground)	5	GND (ground)
Unused	6	Unused
CTS (clear to send)	7	RTS (request to send)
RTS (request to send)	8	CTS (clear to send)
Unused	9	Unused

Note: The left hand column pin assignments are for the female DB-9 connector on the access point. Pin 2 (TXD or "transmit data") must emerge on the management console's end of the connection as RXD ("receive data"). Pin 7 (CTS or "clear to send") must emerge on the management console's end of the connection as RTS ("request to send").

Serial Cable Signal Directions for DB-9 Ports

DB-9 to DB-9 AP		Terminal or PC
1		5
2	Reserved	4
3	←	3
4	→	2
5	Reserved	1
6	Reserved	9
7	←	8
8	→	7
9	Reserved	6

Appendix C
Specifications

General Specifications

Maximum Channels
802.11b/g:
FCC/IC: 1-11, ETSI: 1-13, France: 10-13, MKK: 1-14

Maximum Clients
64

Operating Range
See “Maximum Distance Table” on page A-4

Data Rate
802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11b: 1, 2, 5.5, 11 Mbps per channel

Modulation Type
802.11g: CCK, BPSK, QPSK, OFDM
802.11b: CCK, BPSK, QPSK

Network Configuration
Infrastructure

Operating Frequency
802.11b/g:
2.4 ~ 2.4835 GHz (US, Canada, ETSI)
2.4 ~ 2.497 GHz (Japan)

Power supply
Input: 100-240 AC, 50-60 Hz
Output: 3.3 VDC, 4A
Power consumption: 13.2 watts

PoE (DC)
Input voltage: 48 volts, 0.27A, 12.96 watts

Note: Power can also be provided to the access point through the Ethernet port based on IEEE 802.3af Power over Ethernet (PoE) specifications. When both PoE is provided and the adapter is plugged in, PoE will be turned off.

Physical Size
21.83 x 13.73 x 3.27 cm (8.60 x 5.40 x 1.29 in)

Weight
0.80 kg (1.76 lbs)

LED Indicators
PWR (Power), LAN(Ethernet Link/Activity), WLAN(Wireless Link/Activity)

Network Management
Web-browser, RS232 console, Telnet, SNMP

Temperature
Operating: 0 to 40 °C (32 to 104 °F)
Storage: 0 to 70 °C (32 to 158 °F)

Humidity
15% to 95% (non-condensing)

Compliances
IEC 61000-4-2/3/4/6/11

EMC Compliance (Class B)
FCC Class B (US)
ICES-003 (Canada)
VCCI (Japan)
RCR STD-33A

Radio Signal Certification
FCC Part 15.247 (2.4GHz)
FCC part 15 15.407(b), CISPR 22-96
RSS-210 (Canada)
EN 55022, EN55024, EN 300.328
EN 300 826, EN 61000-3-2, EN61000-3-3
ETSI300.328; ETS 300 826 (802.11b)
MPT RCR std.33 (D33 1~13 Channel, T66 Channel 14)

Safety
CSA/NTRL (CSA 22.2 No. 950 & UL 1950)
EN60950 (TÜV/GS), IEC60950 (CB)
LVD/EN 60950

Standards
IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX,
IEEE 802.11 b, g

Sensitivity

IEEE 802.11g	
Data Rate	**Sensitivity (dBm)**
6 Mbps	-88
9 Mbps	-87
12 Mbps	-86
17 Mbps	-85
24 Mbps	-81
36 Mbps	-77
48 Mbps	-72
54 Mbps	-70

IEEE 802.11b	
Data Rate	**Sensitivity (dBm)**
1 Mbps	-93
2 Mbps	-90
5.5 Mbps	-90
11 Mbps	-87

Transmit Power

IEEE 802.11g	Maximum Output Power (GHz - dBm)		
Data Rate	**2.412**	**2.417~2.467**	**2.472**
6 Mbps	20	20	18
9 Mbps	20	20	18
12 Mbps	20	20	18
18 Mbps	20	20	18
24 Mbps	20	20	18
36 Mbps	18	19	17
48 Mbps	17	16	15
54 Mbps	15	14	13

IEEE 802.11b	Maximum Output Power (GHz - dBm)		
Data Rate	**2.412**	**2.417~2.467**	**2.472**
1 Mbps	15	16	15
2 Mbps	15	16	15
5.5 Mbps	15	16	15
11 Mbps	15	16	15

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

A networking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A group of computers connected as an independent wireless network, without an access point.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Basic Service Set (BSS)

A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using 802.1x dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

Extended Service Set (ESS)

More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.

Extensible Authentication Protocol (EAP)

An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1x port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the access point, and the a RADIUS server

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.11b

A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Infrastructure

An integrated wireless and wired LAN is called an infrastructure configuration.

Inter Access Point Protocol (IAPP)

A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (ODFM)

OFDM/ allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Power over Ethernet (PoE)

A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of access point's and network devices, and significantly decreased installation costs.

RADIUS

A logon authentication protocol that uses software running on a central server to control access to the network.

Roaming

A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

RTS Threshold

Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Wi-Fi Protected Access

WPA employs 802.1x as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA Pre-shared Key (PSK)

PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.

Index

A

Advanced Encryption Standard *See* AES
AES 5-56
antennas, positioning 2-4
authentication 5-12, 6-82
  configuring 5-12, 6-82
  MAC address 5-13, 6-54, 6-55
  type 5-47, 6-76

B

Basic Service Set *See* BSS
beacon
  interval 5-43, 6-78
  rate 5-43, 6-79
BOOTP 6-69, 6-71
BSS 3-3

C

cable
  assignments B-1
  crossover B-3
  straight-through B-3
channel 5-42, 6-77
channels, maximum C-1
Clear To Send *See* CTS
CLI 6-1
  command modes 6-6
clients, maximum C-1
command line interface *See* CLI
community name, configuring 5-25, 6-35
community string 5-26, 6-35
configuration settings, saving or restoring 5-32, 6-42
configuration, initial setup 4-1
console port 1-5
  connecting 2-5
  pin assignments B-4
  required settings 4-2
country code
  configuring 4-4, 6-18
crossover cable B-3
CSMA/CA 1-1
CTS 5-44, 6-81

D

data rate, options C-1
default settings 1-9
device status, displaying 5-61, 6-33
DHCP 4-8, 5-6, 5-7, 6-69, 6-71
distances, maximum A-4
DNS 5-7, 6-68
Domain Name Server *See* DNS
downloading software 5-30, 6-42
DTIM 5-43, 6-79
Dynamic Host Configuration Protocol *See* DHCP

E

EAP 5-54, 6-90
encryption 5-47, 5-49, 5-55, 6-83
Ethernet
  cable 2-4
  port 1-5
event logs 5-66, 6-27
Extensible Authentication Protocol *See* EAP

F

factory defaults
  restoring 5-32, 6-14

filter 5-20, 6-54
  address 5-12, 6-54
  between wireless clients 5-22, 6-60
  local bridge 5-22, 6-60
  local or remote 5-12, 6-57
  management access 5-22, 6-61
  protocol types 5-22, 6-62
  VLANs 5-20, 6-98
firmware
  displaying version 5-31, 6-34
  upgrading 5-30, 5-31, 6-42
fragmentation 6-80

G

gateway address 4-3, 5-7, 6-2, 6-69

H

hardware version, displaying 6-34

I

IAPP 6-97
IEEE 802.11a 1-1, 5-40, 6-68
  configuring interface 5-41, 6-68
  maximum data rate 5-43, 6-76
  radio channel 5-42, 6-77
IEEE 802.11b 5-40
IEEE 802.11f 6-97
IEEE 802.11g 5-40
  configuring interface 5-41, 6-68
  maximum data rate 6-76
  radio channel 6-77
IEEE 802.1x 5-54, 6-50
  configuring 5-14, 6-50
initial setup 4-1
installation
  hardware 2-1
  mounting 2-1
IP address
  BOOTP/DHCP 6-69, 6-71
  configuring 4-3, 4-8, 5-6, 6-69, 6-71

L

LED indicators 1-4
lock, Kensington 2-3
log
  messages 5-35, 5-66, 6-24
  server 5-34, 6-24
login
  CLI 6-1
  web 4-5
logon authentication
  RADIUS client 5-13, 6-45

M

MAC address, authentication 5-13, 6-54, 6-55
maximum data rate 5-43, 6-76
  802.11a interface 5-43, 6-76
  802.11g interface 6-76
maximum distances A-4
MDI, RJ-45 pin configuration 1-5
mounting the access point 2-1
multicast cipher 5-57, 6-88

N

network topologies
  infrastructure 3-3
  infrastructure for roaming 3-4

O

OFDM 1-1
open system 5-47
operating frequency C-1

P

package checklist 1-2
password
  configuring 5-28, 6-22
  management 5-28, 6-22
pin assignments
  console port B-4
  DB-9 port B-4
PoE 1-6
  specifications C-2
power connection 2-4
Power over Ethernet *See* PoE
power supply, specifications C-2
PSK 5-55, 6-91

R

radio channel
  802.11a interface 5-42, 6-77
  802.11g interface 6-77
  configuring 4-7
RADIUS 5-9, 5-54, 6-45
RADIUS, logon authentication 5-13, 6-45
Remote Authentication Dial-in User Service *See RADIUS*
Request to Send *See* RTS
reset 5-32, 6-14
reset button 1-6, 5-32
resetting the access point 5-32, 6-14
restarting the system 5-32, 6-14
RTS
  threshold 5-43, 5-44, 6-81

S

security, options 5-47, 5-48
session key 5-15, 5-16, 6-53
shared key 5-50, 6-84
Simple Network Management Protocol *See* SNMP
Simple Network Time Protocol *See* SNTP
SNMP 5-25, 6-35
  community name 5-25, 6-35
  community string 6-35
  enabling traps 5-26, 6-37
  trap destination 5-26, 6-38
  trap manager 5-26, 6-38
SNTP 5-37, 6-28
  enabling client 5-37, 6-29
  server 5-37, 6-28
software
  displaying version 5-30, 5-61, 6-34
  downloading 5-31, 6-42
specifications C-1
SSID 5-4, 6-78
  configuring 4-6
SSID broadcast 6-75
startup files, setting 6-41
station status 5-64, 6-96
status
  displaying device status 5-61, 6-33
  displaying station status 5-64, 6-96
straight-through cable B-3
system clock, setting 5-37, 6-30
system log
  enabling 5-34, 6-24
  server 5-34, 6-24
system software, downloading from server 5-30, 6-42

T

Telnet
  for managenet access 6-2
Temporal Key Integrity Protocol *See* TKIP
time zone 5-37, 6-32
TKIP 5-55, 6-88
transmit power, configuring 5-42, 6-86
trap destination 5-26, 6-38
trap manager 5-26, 6-38
troubleshooting A-1

U

upgrading software 5-30, 6-42
user name, manager 5-28, 6-21
user password 5-28, 6-21, 6-22

V

VLAN
  configuration 5-20, 6-99
  native ID 5-20, 6-100

W

WEP 5-49, 6-83
  configuring 5-49, 5-50, 6-83
  shared key 5-50, 6-84
Wi-Fi Protected Access *See* WPA
Wired Equivalent Protection *See* WEP
WPA 5-54, 6-91
  authentication over 802.11x 5-57, 6-90
  pre-shared key 5-57, 5-58, 6-92, 6-93
WPA, pre-shared key *See* PSK

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481

From Europe: Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com

Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:
http://www.smc.com
http://www.smc-europe.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-91-352-00-40;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	216-712-36616;	Fax 216-71751415
North West Africa:	34 93 477 4920;	Fax 34 93 477 3774
CIS:	7 (095) 7893573;	Fax 7 (095) 789 35 73
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 6 238 6556;	Fax (65) 6 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-45-224-2332;	Fax 81-45-224-2331
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91-22-8204437;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com, www.smc-europe.com, or www.smc-asia.com.

SMC®
Networks

38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC2552W-G
Pub. Number: 149100022700E, E042004-R01